Online sociological research: methods, ethics and the law

Christian Gerstner

A thesis submitted in partial fulfilment of the requirements of Keele University, Stoke-on-Trent for the degree of Doctor of Philosophy in Sociology

June 2013

Keele University

Abstract

This thesis offers a comprehensive examination of the dilemmas posed by cyberspace for contemporary social research and in how far current ethical frameworks can manage the risks that may emerge in this new research environment. The study is situated in the period of 1998 to 2010, during which the social uses of rapidly converging technological tools led to the extension of the social world into a new social sphere of social interaction called cyberspace. Social scientists have been quick to explore this sphere; however, as the dominant discourses are based on ideas of newness and difference there is uncertainty over what kind of space it is, whether we can transfer existing methods and ethics and what rules apply in the conduct of research.

The thesis first investigates the extent to which the technological tools and ethical dilemmas encountered in cyberspace are in fact new or different. This then necessitates a detailed engagement with the conceptualisation of cyberspace. Thereafter it closes a gap in dominant conceptualisations of cyberspace by offering insights into its legal and regulatory foundations. Next, the thesis reflects on legislation and regulations to identify emerging risks that emerge in everyday social research practice in the online environment. These risks are then used as vignettes to test current ethical guidance's ability to manage them.

The thesis argues that disciplines within the social sciences need to be continually reflexive about their encounters with new spaces, and concludes that cyberspace demands significant engagement with the difficulties posed by the rapid pace of

change of technological development and regulatory and legislator foundations in order to manage risk in online social research. Thus while online research is the focus, the potential of this thesis is to offer a historical insight into the reflexivity of the discipline in particular in how successfully it encounters new spaces of/for research.

Acknowledgements

I am indebted to Helen as she fulfilled the roles of wife, best friend, 'editor', writing manager, fan, jostler, and sounding board with immense love, commitment and saint-like patience. I also thank my parents and sister as they along with Helen kept me going.

Further debt of gratitude is owed to my supervisors Graham Allan and Rebecca Leach who never ceased to challenge my ideas and pushed me to be a better sociologist.

I would like to thank all of those friends and fellow PhD students, who have endured listening to my ideas, reading different versions, made helpful comments and put up with my bouts of panic attacks, absent mindedness and enthralment with everything to do with cyberspace. Deserving a special mention are Lucy, Chaz, Kev, and Fiona.

I dedicate this thesis to my daughters Lillian Joan and Elisa Bronwyn who henceforth have their Daddy back.

Table of Contents

List of Acronyms

Association of Internet Researchers (AoIR)
American Association for the Advancement of Science (AAAS)
American Sociological Association (ASA)
American Psychological Association (APA)
Bundesnachrichtendienst (BND)
British Sociological Association (BSA)
Computer-mediated communication (CMC)
Cyberspace Research Unit (CRU)
Data Protection Act (DPA)
Electronic Frontier Foundation (EFF)
Economic and Social Research Council (ESRC)
European Union (EU)
Federal Communications Commission (FCC)
Information Commissioner's Office (ICO)
Instant Messenger Service (IMS)
International Corporation for Assigned Names and Numbers (ICANN)
International Sociological Association (ISA)
Internet Service Provider (ISP)
Master Control Programme (MCP)
Multi-user Dungeon (MUD)
Microsoft Network (MSN)
National Science Foundation Network (NFSNET)
National Society for the Prevention of Cruelty to Children (NSPCC)
The National Committee for Research Ethics in Science and Technology (NENT)
Personal Identifiable Data (PID)
Personal Identifiable Information (PII)
Regulation of Investigatory Powers Act (RIPA)
Real life (RL)
Reduced Social Cues model (RSC)
Socially Desirable Response (SDR)
Social Identity Deindividuation model (SIDE)
Sociology of Cyber-Scientific Knowledge (SCSK)
Social Research Association (SRA)
Socio-technical-legal theory (STL)
Undesired bulk electronic messages (SPAM)
Telekommunikationsverordnung (TKUV)
United Nations (UN)
Virtual Reality (VR)
World Wide Web (WWW)

Chapter 1:

An evolving thesis

1.0 Introduction to the study

This thesis is an exploration of how social science as a discipline engages with ethical and legal dimensions of a 'new' research environment and tests/reviews how capable current ethical guidance available to social researchers is in managing the perceived and real risks to researchers and their respondents in online sociological research.

The research focused on the period of time between 1998 and 2010, when there was a considerable development of communication tools and their convergence into what is called the Internet and cyberspace. It is a time when more and more business is done online, and when individuals are encouraged to spend increasing amounts of time in online social activities. The latter refers in particular to social media such as MySpace, Facebook, YouTube and various chatrooms and instant messengers. This is picked up by one of the most influential contemporary sociologists, Castells. In his body of work (1996, 1997, 1997, 2005) he engages with the fundamental changes in social life by offering a meta account of what he terms the network society. His hypothesis is that a new society has begun to emerge through the restructuring of the economy by a complex interplay of technological developments and non-linear evolutionary opportunistic integration thereof. This new society is manifested in the transformation of sociability

creating a hypersocial society (Castells, 2005). Castells argues that "people fold the technology into their lives, link up virtual reality and real virtuality, they live in various technological forms of communication, articulating them as they need it" (2005:36). This means that the social and sociological study of this new network society is crucially important in order to make sense of everyday experiences. This in turn was taken up by many fellow researchers as a call to research and we see a considerable increase in the online environment being considered worthy of study (Hine, 2004).

This study itself emerged out of my initial research project where I tried to do online social research within existing ethical guidelines, yet it appeared at the time that these ethical guidelines were not sufficient in protecting me as a researcher due to the perceived risky nature of the chosen research environment. A strong sense developed that people think that cyberspace and the Internet are not just new research environments but are actually new and different spaces of social interaction that create new ethical dilemmas for social research and make current ethical guidance obsolete. Thus this chapter contextualises and begins to theoretically ground the study by outlining its emerging nature and exploring understandings of ethics and risky research. In the following chapters of this thesis I first investigate the newness and difference debates surrounding cyberspace, the internet and online social research. The next chapters offer an insight into the impact of this battleground of newness and difference on (online) social research. The thesis then moves on to provide social scientists with a model for understanding the legal conceptualisation and creation of cyberspace. I

then assess in detail the impact of legislation and regulation on online social research; evaluate the ability of current ethical guidance to manage the identified risks; and conclude by offering a possible implementation framework for online social research ethics.

1.1 An evolving research project

In 2003 I began work on a PhD research project entitled "Family money: the uses of money in familial relationships". Of particular interest were intergenerational familial relationships and how money was constructed, negotiated, transformed, and earmarked to reflect the nature, direction, and inner workings of those relationships. Within the first year a literature review was written, a clear methodology was planned and I was ready to commence with the empirical part of my research project. The study's ontological and epistemological position understood children/ adolescents as 'human beings' rather than 'human becomings' and supported feminist ideas of empowerment (Lee, 2005). Thus, there was a clear sense that the research may be negatively influenced by either not being able to gain access to children due to parents preventing it, or children's opinions being heavily vetted by their parents. This concern was grounded in the research findings of my MA thesis on the meanings of money in English society which suggested that adults do not like talking about their money dealings. They liked it even less when their children could hear this 'money talk' or would be asked for their own opinions directly.

In this context it became clear that a methodological approach had to be devised that circumvented these issues. In response to this it was decided to use a mixed approach which, as well as 'offline' interviews, would also include online research tools. Apart from the practical advantages, the underlying rationale for the use of Internet technologies was that I could interview teenagers via the Internet using several different technologies (i.e. email, IMS, online questionnaires). This makes their voices heard in a way that was closer to their real feelings, while avoiding fear of parental disapproval or censorship (Holloway and Valentine, 2003; Katz, 1998). Additionally, I hoped to gain access to teenagers who would not normally talk to social researchers or who would, more often than not, be difficult to gain access to.

There were some important issues to consider when deciding on the means of the initial approach of potential participants online. As other researchers have found (Stern, 2004; Bober, 2004) one example of such issues is that of gaining informed consent. US law (US COPPA, 1998) at the time considered teenagers the 'personal property' of their parents up to the age of 18 – making it inappropriate for me to contact the underage part of my sample without prior parental consent. At the same time in EU countries young people of the age of 16 and above - as long as they are judged competent - can give their informed consent (UK DPA 1998, Children Act 2004, UK).

In response to this I developed a research website that was publicly accessible and provided all the key information on me as a researcher, the research project,

contact details and potential participant's rights. Furthermore, the website permitted those interested to use an online form to contact me in order to ask for further information about the project or to declare their interest in participation. The website was designed in this way because by respondents contacting me I was able to successfully address some of the legal and ethical issues of consent. On the practical side the form was structured in a way that made it clear that I only accepted participants of the age of 16 and above. The website link was to be placed on moderated messaging boards and websites of respectable organisations (e.g. NSPCC) to give the project further credibility.

During the PhD progress meeting at the end of the first year several issues where considered and all but one was resolved satisfactorily. The issue was that senior academics of the panel disagreed about the potential impact that child protection and the perceived dangers posed by cyberspace could have on my chosen approach. They acknowledged that while my research project would not have put children at risk, child protection issues at the time and the ways in which they were understood and addressed in the context of the Internet and cyberspace, posed a big obstacle to my methodology. I was informed by members of the panel that even though my ethical considerations and methodological arguments were both sound, in the context of the time, carrying out the research could have had a detrimental impact by bringing about a problematic starting point for my academic career. This suggested that while being a 'good' researcher who followed ethical guidelines and methodological theory correctly and in a novel way, I was not able to carry out the planned research.

1.2 Risky social research

The question that I was left with was why did ethical and methodological guidance not permit me to take research design and action decisions that would protect me as a researcher from the identified risk. This led to two further questions:

- Is this even the role of ethics guidance?
- What makes research sensitive or risky research?

1.2.1 To serve and protect?

In order to understand contemporary positions on ethics and their role in research I reviewed their origins and then moved to a closer consideration of my particular dilemma. There are 6 ethical traditions: Indian, Buddhist, Classical Chinese, Jewish, Christian and Islamic that are dominant around the globe. In terms of Western ethics, these are founded on two key traditions – Greeks and Hobbes/ Rousseau and Christianity (Rowe, 1993). Migley (1993) distinguishes between these two influences through their originating myths. Greeks and Hobbes/ Rousseau are built on the idea of a social contract; while Christianity's origin myth is the 'fall of man'. Ideas of a 'social contract' became particularly prominent during the Enlightenment. Preston (1993) informs us that within Christianity, Protestants use 'ethics' and Catholics use 'moral theology'. Nevertheless both are concerned with the same two basic issues in ethics: a) how to act from the right motive; and b) how to find what is the right action in particular circumstances (Preston, 1993). In this they are not actually different from moral philosophy apart from their respective starting points – namely Christian faith; or humanism.

Schneewind (1993) argues that modern moral philosophy developed in three stages. Stage one involved a shift from thinking that morality has to be imposed on human beings to it being understood as self-governance. This stage is exemplified by the works of de Montaigne (1595) and Kant (1785). To surmise it is the shift from the idea of natural laws presented to the reader through the works of Aristotle and Plato to the notion of moral law developed principally by Kant (O'Neill, 1993; Buckle, 1993).

In natural law "human moral beliefs have a rational foundation, in the form of general principles of right and conduct that reflect a determinate and rational human nature" (Buckle, 1993:173). Kantian ideas believe in human freedom and that moral obligation derives neither from God nor from human authorities and communities, nor from the preferences or desires of human agents, but from reason (O'Neill, 1993). Stage two was about shoring up this progress. And in stage three we can see a shift in focus from autonomous individuals to new issues concerning public morality (Schneewind, 1993).

In modern times there was a dominant practice, quite contrary to Kantian positions on morality, that humans needed to be told how to behave in order to avoid doing wrong (Bauman, 1993). The key way in which this was achieved was through the link between the work of legislating authorities and moral philosophers. Bauman (1993) offers this insight when he argues that their co-operation was based on the "twin banners of universality and foundation"

(Bauman, 1993:8). Legislators constructed universality as one corpus of legislation that extended over a particular locality. Philosophers for their part "defined universality as that feature of ethical prescriptions which compelled every human creature, just for the fact of being a human creature, to recognise it as right and thus to accept it as obligatory" (Bauman, 1993:8).

In this legislators' practices provided a foundation for moral philosophers to build their models of universal human nature. In doing so the cultural artefacts became transformed into naturalised realities and seen as the quintessence of human destiny (Bauman, 1993). Simply put, legislation created the foundation for moral philosophers to develop ethical positions that were reinforced by the coercive power of said legislation, while legitimising the legislation by removing the cultural trace of particular locality and making them universally accepted laws and ethics by which members of that society live.

Events at the end of the 19th and the beginning of the 20th centuries have, however, shaken the belief in the strength of our legal and moral codes at the time, and maybe our human ability to self-regulate our actions. Thus in the middle of the 20th century we see a drive to strengthen the legal and moral understandings of ethical actions. This is also the point at which we begin to see a drive to critically engage with research. This latter is born out of a reflection on the atrocities perpetrated by the Nazi regime during the Second World War and laid the foundations for legislating the ethical conduct of medical researchers.

Consequently, in 1949 we see the creation of the Nuremberg Code, which amongst other things instructed that all research involvement has to be voluntary. Legislators and regulators were not satisfied with this sole provision, in part due to subsequent continued learning through poorly conducted research occurrences. Hence, in 1964 the Declaration of Helsinki, with a particular focus on biomedical research, further developed the principles enshrined in the Nuremberg Code. It introduces notions such as weighing the risk vs. benefit of research, the need to respect the subject's privacy and set out to minimize the costs of participation to the subject (Kitchener and Kitchener, 2009).

This was then followed by specific countries, especially the US, developing their own legislation and expert authorities to create a legal-ethical framework within which researchers were required to act. From there we witness the development of professional associations and their professional code of conducts; university ethics boards and their own institutional codes of conduct; and institutional ethics boards and code of conducts – creating ethical frameworks with increasing specificity to particular locations and research topics and participants (Speiglman and Spear, 2009).

The way in which moral behaviours and I propose thus ethical guidelines were constructed they, as legislation, did strive to "define the 'proper' and 'improper' actions in situations on which it takes a stand. It sets for itself an ideal […] of churning up exhaustive and unambiguous definitions; such as would provide clear cut rules for the choice between proper and improper and leave no 'grey-area' of

ambivalence and multiple interpretations" (Bauman, 1993: 11). Beyond that the ways in which ethical guidelines were aligned with or subsequently revised in line with legislation (i.e. Data Protection Acts etc…); established clear sanctions if they were broken. This provides further evidence for Bauman's (1993) argument that legislation and moral philosophers' actions reinforced each other and not only created a societal/ national moral code of behaviour and sanctions, but a whole new subset or extension thereof into the arena of medical and then also social research.

This created ethical guidance for social research that by an large is based on the premise that a) each discipline can develop a set of rules of engagement that apply for any possible number of research contexts; b) that following the rules will ensure a fair balance of rights, benefits and risks and the level of possible harm; c) that researchers themselves cannot self-regulate but are only able to carry out research safely if they adhere to these guidelines. Punishment for failure to do so would lead to harming the research subject and depending on the severity thereof, lead to legal and/or professional consequences for the researcher.

In a way this offers a rather comforting position to a researcher. One will be able to carry out research on any topic safely as long as one considers the matters raised in their discipline or institution's ethics guides. It functions as a road map that should lead to high quality research and avoid harm. While learning and reflecting on these developments in ethical research, I felt very much aligned with the principle that ethical guidance's ability and thus role is to enable the

researcher to reflect on their research method and research participants carefully and thus protect all parties from harm. Consequently, when reflecting on my initial research's dilemma I reached a position where I viewed current ethical guidance as failing their raisons d'être. Beyond that, I also knew that despite Bauman's (1993) statements of the symbiosis between law and moral philosophy; in my research context clearly legislation and research ethics did not work together to identify a natural universal ethical framework that if followed avoids harm.

Further investigation showed that the belief that there can be one universal ethical framework is a somewhat idealistic if not unrealistic premise for several reasons. One, even within the research community is a deeply engrained debate about several ethical principles. One example is debates about where the line between benefit and risk should be drawn. This is particularly the case in debates concerned with covert research (Dingwall, 1980; Homan and Bulmer, 1982; Homan, 1992; Punch, 1998). Another area of dispute is that of confidentiality and anonymity (Bostock, 2002; Grinyer, 2002). If one explored these two areas in more depth than is necessary for my arguments here, one would find many examples on both side of the argument that indicate that this sense that there could be one universally agreed interpretation of social contexts and thus moral imperatives is much more challenging than ethics guides themselves indicate.

This latter point is something that postmodern attitudes towards morality are focused on. The dominant discourse within this tradition describes the death of

the ethical or as Bauman writes "the substitution of aesthetics for ethics, and of the 'ultimate emancipation' that follows" (Bauman, 1993:2). One of the underlying reasons for this is that in postmodern times "the once unitary and indivisible 'right way' begins to split into 'economically sensible', 'aesthetically pleasing', 'morally proper'. Actions may be right in one sense, wrong in another" (Bauman, 1993:2). Consequently, postmodernism tells us that there is no chance of a common and empirically founded ethics guide. Everything is relative and has to be negotiated in a temporal, localised and contextual snapshot where one may draw on previous experiences only as a very tentative starting point. In a way it is evidence of the splintering of one dominant modern paradigm of morality into a sheer endless number of possible moral paradigms. This radically reverses the sense of certainty, no matter how unjustified it may have been, that modern ethics guidance has given to researchers.

Bauman (1993) takes a strong position on current ethics guides. He writes "It is the ethical codes which are plagued with relativism, that plague being but a reflection or a sentiment of tribal parochialism of institutional powers that usurp ethical authority" (Bauman, 1993:14). Beyond that he questions how anyone could claim to take moral responsibility when there are so many people involved in any social context in today's world.

In his book Postmodern Ethics (1993) Bauman explores the possible consequences of this postmodern reality for ethics and morality in general, and thus provides an

opportunity to reflect on the role of ethic guidance and its potential format to this study.

One consequence that Bauman (1993) identifies is akin to Weber's (1990) salvation anxiety experienced by Protestants. While Weber points out that Protestants experience moral anxiety because they are responsible for their own salvation as a consequence of removing the priest and permitting a direct relationship with God; in today's world the authorities we used to turn to for moral guidance have become contested. Bauman (1993) draws on ideas of Moore to suggest that the religious 'pluralism' identified by Weber has over time become a moral pluralism. While we are now emancipated to take charge of ethics, we are no longer in a position to rely on ethical guidance to guarantee a positive outcome of our research.

These themes of postmodern anxiety are also present in the works of Giddens (1991) and Beck (1992) who both identify the postmodern time to be so ambivalent as to offer many more opportunities of choice yet at the same time thereby creating a level of uncertainty and ambiguity that postmodern times are often experienced and perceived as risky. Bauman's (1993) reflections on the work by Giddens and Ulrich lead him to draw inferences that resonate with my own research. Not only has the reality of postmodern pluralism created contested authorities another reality of current times that is having a considerable impact is that of a change of social space.

Social space consists of three elements: cognitive, aesthetic and moral. In pre-modern and in many ways modern times, social space was marked by close proximity (Soja, 1996). In late modern and especially postmodern times this proximity has been exploded. Causes are modern means of transportation and communication; and geographical mobility due to labour markets. Thus the morality of proximity is "…woefully inadequate in a society in which all important action is an action on distance…" (Bauman, 1993:217). This globalisation of morality further drives the sense of pluralism. Not only are there several possible moral paradigms from within a particular society/ culture but also from a Western and then global context. In times of technological change, particularly the communication opportunities offered by the Internet and cyberspace, this sense of uncertainty may only be further enforced.

In a way ethics or morality are not so much concerned with crisis management but instead are trying to predict and control the future. Yet, "…with a future that is endemically the realm of uncertainty and the playfield of conflicting scenarios.." (Bauman, 1993:220), this is a difficult undertaking. Jonas (1984) suggests that "future ethics to be guided by heuristics of fear, sub-ordinated in its turn to the principle of uncertainty" (Jonas in Bauman, 1993:220).

These ideas imply that pluralism and ambiguity within each, law and ethics, and between them results in an uncertainty of interpretation of actions (to be) taken in research. This uncertainty relates to the tension between ethics and the law, i.e. that actions may be ethical but illegal, or vice versa; or even unethical and illegal

to some but not to others. Consequently, ethical guidelines themselves have to be understood as temporal localised snapshots of ethical interpretations put forward by a particular interest group that may or may not be in line with relevant applicable legislation. This then suggests the need of a thorough review of current ethical guidelines with view to establish in how far they are able to fulfil their raison d'être in the context of research and in my case online sociological research. To be specific, do current ethical guidelines enable and encourage the online social researcher to a) understand them as temporal and tied to particular contexts; and thus b) to see the need to review anew the 'tension' between ethics and the law in each research instance.

This also then requires me and the reader to acknowledge that my particular understanding of ethics and its derived guidelines is that their purpose is to provide a reflexive framework that guide human behaviour to avoid harm as the lack of this guidance may lead to harm as human behaviour is not naturally ethical but driven by ambiguous interpretations of what is ethical and what is not at that particular temporal and socio- geographical location.

1.2.2 Risky research

The deliberations thus far then also suggest that every research is potentially sensitive or risky. In a world that is ambiguous and thus uncertain, where ethical guidelines cannot simply be relied on at face value, any research interaction becomes a risky negotiation in order to establish appropriate behaviours and communications that avoid harm. However, there are gradients of sensitive and

risky and the field of social research has considered this topic in detail. To address the question of what is sensitive or risky research and what makes it thus, I used my initial research as a tool of reflection to identify particular factors that played a role in making it too risky. To begin with I explored current understandings of what makes social research risky.

What became clear is that the literature does not focus on the kind of risk that I have been confronted with. There are many publications that reflect on sensitive topics (Allmark, 2002; Corden and Sainsbury, 2005; DVRG, 2004), and others that address risk to the integrity of research and researcher and thus the research participant (Adler and Adler, 2002; Bostock, 2002; Gilbert, 2001). The former literature often has a particular focus on how certain topics or methods may affect a particular group of respondents or even the researcher. The latter describes the risks that certain topics and methods pose to researchers or respondent. This body of work discusses matters such as the risk of state intervention to 'abuse' the research data in evidence against the research respondent. It may also address the matter of a researcher's safety while carrying out the research and the danger that the research environment poses.

While reading these sources it transpired, however, that their focus was on possible physical harm to the researcher or the consequences if they did not comply with the request to share information with official bodies. Lee's (1993) seminal work but also preceding publications such as Knerr (1982), Akeroyd (1988) and Polsky (1971) discuss and provide case examples of this.

One particular area in the social sciences that has considered the legal and regulatory risks to a researcher is criminology. Criminologists may enter contexts that provide them with information that may either make them witness to illegal activity or actually even implicated by association. There is a lot of debate and a readily identifiable dichotomy between those who draw a clear line by not entering these research contexts as their interpretation of ethics and legislation prevent them; yet reversely there are many who as Akeroyd (1988) states simply opt out of certain legislation to avoid inopportuneness. This latter group is subject to risks that are the type of risk that was identified in relation to my initial research. I equate them because they present a similar tension between the law and ethics and the possible 'unintended' legal consequences caused by 'ethical' actions.

I propose two things: 1) that there was a time where the research context was rather more constrained in geography. By this I mean that the criminologist would be able to readily identify legislation and regulation that may impact on their research and that the majority would have done so due to the methodological and particularly ethical discourse within the field. 2) that increasing globalisation and especially the growth of the internet alongside this has dramatically affected the ability to be cognisant of all the legislation and regulation that applies to one's research and research context. If one choses the position of 'opting-out' then that considerably increases the risk to the researcher, because their actions may well break legislation and regulation.

What is not discussed in depth across the social research literature is how a particular research environment may have legal and regulatory realities which potentially interact with our ethical guidelines in contradictory ways. The exception to this statement is research on vulnerable groups, principally that on children. Work by Alderson (2000) and Stern (2004) offers a particularly useful example of the need to make the connection between ethics and legislation/ regulation of a specific research context to continuously create up-to-date research guidance and thus practice which moves research from risky to 'risk managed'. At this point my reflections on risky research further enforced my position that we cannot rely on static ethics guidance or understandings of legal and cultural research contexts but have to continuously update our knowledge thereof in order to manage the risk in a way that it does avoid harm and permits valuable research to go ahead. This then implies that current ethical guidelines are 'out of kilter'.

This understanding and reading Alderson's body of work encouraged me to undertake a deeper reflection to unpack the child protection issues that had such a big impact on my original research and looked at ways of managing the at least perceived risks to social researchers by applying current ethical guidance. This approach is in line with the belief that ethical guidance's purpose is to shield all those in research from potential harm.

There were two key areas of development that put pressure on ethics guidance in my initial study: a) child protection; and b) perceptions of cyberspace. The thesis

was undertaken at a time when there was a particular public and political focus on child protection issues. Two examples of issues of concern were: ensuring that only suitable adults worked with children, and the need to improve child protection procedures of social services (Children Act 2004, UK). The focus on these issues stems from an increase in the reporting of children as victims of crime, suggested failures of child protection procedures, and public demand for a determined response. The outcome of this focus was an increase in police activity such as operation 'Paladin Child', an increase in child protection organisations' activities such as Childline and increased formalised involvement with the police and social services; and an increase in legislation such as the 'Protection of Children Act (Scotland) 2003' and the 'Children Act 2004' (UK).

While these child protection issues were being raised there was a growing public and political debate about the Internet and cyberspace. This debate occurred mainly in/through the news media and appeared to be focusing on 'the dark side' of the Internet and cyberspace. Even reputable news media used exaggeration and prediction as tools in their reporting. Examples of headlines in the Times newspaper from the year 2003 are: 'Terrorists use internet to plot gang warfare' (Adams, 2003); 'Internet pirates provoke identity crisis of luxury brands' (Mortishead, 2003); 'Police will run internet after terrorist attack' (Leppard, 2003). While this way of writing on the Internet painted a much darker picture of the medium than I expected, it was the following headlines that were to become of particular importance to me: 'Internet pervert who groomed girls jailed for 5

years' (McGrory, 2003), and 'An amnesty for internet paedophiles? (Wheeler, 2003).

This understanding of cyberspace prompted several responses from the private and public sectors. Child protection/ interest groups began to develop advice on how to use the Internet safely for both parents and their children. A good example of this is the NetSmartz workshop by the National Center for Missing and Exploited Children. The next step for them was to monitor Internet communications and become the main recipient for complaints about indecent materials. Internet service providers (ISP) started to create safe children friendly online environments. Governments created a whole range of laws to tackle online child protection issues. These will be discussed in detail in chapters five and six. Last but not least police forces around the world have worked very closely to 'clean up' cyberspace. One indication of their activities are the frequent reports in the media of the successful routing of paedophile networks.

At this point my deliberations had led me to understand that there is a complex potential connection between child protection issues, the way we understand cyberspace and the possible link that may exist between them and online social research. The researcher going on the Internet to find adolescents to ask them personal questions about themselves in an environment that is not perceived as safe is, for them ethically problematic. Additionally, I as a male fall into the category of the most likely source of that danger. In the climate outlined above it would be no surprise for parents, child protection groups, police forces,

governments and adolescents themselves to be highly suspicious of, and even quick to 'sentence', a stranger online. I became aware that my online activities would be received highly critically and that I would have to work hard to earn trust but to also protect myself from potential false allegations that may arise out of misunderstandings.

1.3 The problem statement

My reflections and research have led me to realise that the matter that I had been dealing with throughout is that of managing perceived and real risk in social research environments/ contexts. The risk to my research's data; to my research participants; to me as a researcher that are brought about by the ways in which my chosen research environment and topic where constructed, understood, used and responded to.

In this light my research focus began to shift to the overarching issue of how social science ethical guidance engages with new areas and environments of social research and the researcher's ability to negotiate difficult research matters by applying this guidance. Thus, in 2005 I agreed with my supervisors that the matter of how social science engages with and attempts to manage this risk in the context of online social research, and its apparent failure to do so in my initial research, is so important as to justify abandoning my initial project.

Therefore the topic of research of this thesis is:

"How successful is current social research ethical guidance in managing potential risk in the context of online social research?"

The research objectives of this thesis are to:

1) Identify dominant conceptualisations of the Internet and cyberspace as research contexts within social research.
2) Unpack the legal and regulatory conceptualisation of the Internet and cyberspace.
3) Document and analyse current legislation and regulations which are relevant to social research on/ or via the Internet and assess their potential impact on current research guidance and practice.
4) Critically evaluate ethical guidance in the context of the emerging legal and regulatory Internet and cyberspace to ascertain how suited they are to managing risk in online social research.

1.4 Methodological overview

The investigation of this study was undertaken using two methods 1) a library based study of current ethical guidance of social research; and legislation and regulation of the Internet and cyberspace. 2) constructing a range of 'worst case' scenarios that could emerge out of possible routine social research actions within the legal and regulatory nature of the Internet and cyberspace; and current ethical and conceptual understandings of the Internet and cyberspace. These were then used as the context within which I tested the currently available ethical guidance.

The matter of using worst case scenarios in my project may be a controversial choice in particularly as in the context of my initial research any ethical dilemmas and tensions between the law and ethics were all hypothetical. They were hypothetical as I had to speculate on potential scenarios as there was no published evidence of any online social researcher being sued, investigated or arrested due to perceived or actual improper conduct. This was further confirmed by my general arguments and conference presentations being questioned as to why I was using worst case scenarios and that no online researcher had been known for getting 'into trouble' yet. Colleagues wanted to receive a more nuanced "what is actually likely to happen in 'mundane' research interactions" engagement with my topic.

Reasons for persisting with the use of worst case scenarios will be outlined in the following section. I argue that it is important for social science to engage with this topic because as a reflexive practice we have to continuously consider how we engage with our research environments in terms of how we conceptualise them as spaces and possible interactions within them; and how we thus respond to them in our methodological and particularly ethical approaches/ guidance. The application of worst case scenarios offers a means to test current guidance's ability to manage risk. The rationale here is that I argue that if an ethical framework can manage worst case scenario risk in research then it can easily manage mundane activities.

My own experience in my initial research project suggests that a risk adverse panel based its assessment of my proposals on worst case hypothetical scenarios and their concerns arose out of an inability of current ethical guidance managing this perceived hypothetical risk. This also implies that wider social research identifies risk and manages this risk in general by identifying worst case scenarios to test the ethical and methodological approach and actions of research. The following example of a hypothetical worst case scenario becoming real

1.4.1 The age of Paranoia?!

At this point I offer a case study of events that began in 2008 and are still reverberating in 2012. The aim is to use this case as a) an illustration of why it is important to be committed to reflexively engage with online social research risks and methodological, particularly ethics guidance; and b) to justify the use of worst case scenarios. Far from paranoia, my position as outlined above is that ethical and methodological guidance should enable researchers to make decisions and choices in their research design, approach and actions that avoid ending up in worst case scenario situations and if they end up in one after all to enable a clear route out. Before proceeding, I offer a brief disclaimer that the following case study is not offered to discuss guilt of any parties or to make a political point.

In 2008 the press and the Internet became sites of intense discussion about the "Nottingham Two". Nottingham University's School of Politics and International Relations is known for its research and teaching on terrorism related matters.

'Nottingham Two' refers to two researchers from the University of Nottingham, one a member of staff and the other a PhD student.

In 2008 the PhD student downloaded an Al-Qaeda training manual from the US Justice Department website as part of literature that he was using to prepare his PhD proposal. In this activity he was assisted by his aforementioned friend who worked at the University of Nottingham as an academic member of staff. The Al-Qaeda training manual was noticed on the latter's computer by a colleague who reported it to the university, who then in turn reported this to the police. This resulted in a police operation called "Minerva" and led to the arrest of the academic member of staff under the 2000 Terrorism Act. When the PhD student tried to support his friend and explain why they had this document, he was also arrested. They were both released after one week of imprisonment. After the release, Sir Colin Campbell, then Vice-Chancellor of the University, explained his and the university's actions:

> "There is no 'right' to access and research terrorist materials. Those who do so run the risk of being investigated and prosecuted on terrorism charges. Equally, there is no 'prohibition' on accessing terrorist materials for the purpose of research. Those who do so are likely to be able to offer a defence to charges (although they may be held in custody for some time while the matter is investigated)" (Newman, 2008).

Following this incident the university and its then Vice-Chancellor were heavily criticised for what was perceived as a failure to support legitimate research activities from undue threat of the Terrorism Act. This criticism was further strengthened when the university's Politics Department set-up a module review committee to review the reading materials of its staff and modules to identify "material that is illegal or could incite violence" (Newman, 2009).

David Miller, professor of sociology at the University of Strathclyde and the convenor of Teaching About Terrorism, said

> "Nottingham's review policy represented a fundamental attack on academic freedom. The module review committee is a censorship committee: it can't operate as anything else. The university is acting as the police, one step removed" (Newman, 2008).

Within the research community and beyond a concern arose that questioned how a relevant research topic (in this case terrorism) could be 'misconstrued' in a way that not only prevented the particular research project but also any future research for fear of potential unintended consequences to the researcher – not for doing anything methodologically or ethically wrong (as per current conventions) but for a lack of meaningful relationship between legislation, politics and research.

A Lecturer from within the 'affected' department commented:

> "We are greatly concerned by the disproportionate nature of the university's response to the possession of legitimate research materials.

> Both the individuals are unreservedly innocent and they and their families and friends and have been greatly distressed by the overzealous police investigation. It is crucial that we do not let concerns for security become the enemy of liberty and academic freedom" (Jackson, 2008).

As a consequence of the perceived lack of protection when undertaking legitimate research Dr Rod Thornton decided to stop teaching the topic of terrorism at the University of Nottingham, which also means that the topic is no longer taught at the university as a whole. Thornton then proceeded to writing and presenting a highly controversial paper outlining his allegations of misrepresentation and misdeeds by the university against its own staff for which he was subsequently suspended. In response to his suspension 67 international researchers wrote an open letter in the Guardian (10th May 2011) petitioning for Thornton's reinstatement and an independent investigation of the university's actions in relation to the initial incident.

Professor Parmar, the Chair of the British International Studies Association wrote an open letter to the then Vice-Chancellor of the University of Nottingham, arguing that there was a "strong feeling of unease and concern across [BISA] over the issue of academic freedom raised by, but certainly not confined to, the ongoing case of Dr Rod Thornton" (www.bisa.co.uk). The letter also called for the University of Nottingham to "consider" supporting an independent inquiry into the allegations and issues raised in Thornton's report (www.bisa.co.uk).

The ways in which the parts of the research community have chosen to respond to these events show that there is still a strong feeling, already identified by Long and Dorn's (1983) investigation, that research should not be regulated by official institutions such as the Police. It also offers further evidence for Lee's statement that "conflict between researchers and regulators has arisen; however, over the form regulation should take" (Lee, 1993:27).

The key points from a pure research point are that a PhD student collected legitimate research data from a trustworthy source, using conventional research methods; and the ethics guidance at the time would have not flagged up any potential risk. The researcher may well have been aware that he was studying a controversial topic, but I am certain that neither he nor the wider research community would have constructed his research approach or actions as 'risky' research. The responses to the university and police's actions provided in the case study further reinforce this point.

What appears to have happened is that there is a detrimental gap between how social research perceived this research environment and activities (as non-risky) and how the university and police perceived those actions at a time when this topic was constructed and perceived as a threat to the status of the institution and society as a whole. Of concern is the fact that both sides were able to evidence that their actions were legitimate. The researcher was able to point to his research methodology and particularly his ethical framework while the university and police were able to point to legislation – particularly the Terrorism Act; to

justify their respective actions. Thus, there is evidence of a tension between ethics guidance and the law that transcends my own initial research topic. This further validates the need to carry out the current study as relevant beyond my topic and my decision to use hypothetical worst case scenarios.

It also suggests that ethical guidance has to do more than provide questions for ethical considerations; it also needs to prompt an engagement with the socio/cultural-legal context of the chosen research environment. There is also a sense that the legal conceptualisation of the research environment and the actions taken within overrides methodological and ethical considerations and perceptions at least in the short-term. I state this because the academics were arrested in the first instance but then released without charge. This may well mean that our current research ethics and methods are appropriate in that they actually did work fine and that it was the interpretation of the law that caused an undue interference with the researcher and his research. This is also in line with findings of Lee (1993) which showed that most researchers who were taken to court for refusing to comply with subpoenas were released without charge. At this point someone may also point out, again, that this is a one off extreme example. Yes it is. However, based on my position on the role and responsibility ethics guidance ought to fulfil, my view is that current guidance failed to protect the researcher from undue threat and actual imprisonment.

Hence, this thesis contains a range of hypothetical scenarios/ vignettes that could emerge out of routine research activities in the interactions between said activities

and the legal and regulatory realities of the online research contexts to assess in how far current ethical guidance manages potential risks in this research environment. I chose to apply a range of scenarios because any one specific case study would not have allowed me to identify the considerable range of issues presented in this thesis.

1.4.2 Document analysis

In order to answer my research question, meet the study's objectives and create the contextual information in to which to apply these worst case scenarios, I carried out a library based study. I chose to conduct my project in this way rather than by means of a questionnaire or interviews of stakeholders such as individual researchers or ethics boards for four main reasons: a) In order to answer my question I did not need an in-depth understanding of researchers' personal views on, or experiences of online social research; b) (because) Those views that inform the debate and that impact on research guidance are all published and readily available through journals and other literary sources; c) Much of the required data was to be drawn from diverse sources (i.e. laws, regulations, ethics guides), all of which were accessible in document form; d) the matter of governance that arises out of decisions of ethics boards in relation to online social research, while critical in research practice outcomes, bases these decisions on the data that I investigate. Thus, rather than being an integral part of this present research, the study of governance through ethics boards is an important area for future research that is based on the findings of this thesis. My research focuses on the investigation of available guidance and how successful it is in managing potential

risk in online social research; future research needs to consider how this guidance is applied in terms of governance of online social research.

The thesis overall has a "photographic model" of structure. Chapters one, two and three provide a broad overview ("wide angle shot") of the context of the thesis and the topic of the thesis in particular. Chapters four to six move to an increasingly closer view of the issue, dealing with the use of legal conceptualisations of cyberspace and zooming in for "close-up shots", considering legislation and regulation and their potential impact on online social research especially in terms of risk; and the appropriateness of current ethical guidance in managing this risk in such a context. Chapter seven reflects on the findings of previous chapters and provides a concise conclusion.

To meet objective 1) Identify dominant conceptualisations of the Internet and cyberspace as research contexts within social research, I review the dominant discourses and conceptualisations of cyberspace and the Internet in social science literature in chapters two and three. Of particular interest are the ways in which the field conceptualises the online research environment and what the proposed consequences for social research are within this context in relations to ethical frameworks. The thesis thereby unearths the dominant positions on cyberspace and the Internet and identifies the key ways in which social science constructs this environment for social research purposes. By doing so it is the first piece of work undertaken to identify one possible reason for the tension between ethics and the law in online social research.

To meet objective 2) Unpack the legal and regulatory conceptualisation of the Internet and cyberspace, I draw on data gathered from academic literature, particularly from the legal profession that defines cyberspace, government statements and legislation and regulation of cyberspace and the Internet; in order to arrive at a legal understanding of cyberspace. I use this data in chapter four to identify the direct and indirect legal and regulatory definitions of the Internet and cyberspace. By undertaking this work the thesis contributes to social sciences' understanding of the nature of cyberspace and the Internet, adding a crucial facet to its conceptualisation of cyberspace which as shown in chapters two and three relies heavily on cultural understandings and does not pay necessary attention to this basis of cyberspace and the Internet. Acknowledging the fundamental legislative and regulatory foundation to our cultural understanding of cyberspace offers a full appreciation of this research environment permitting an accurate assessment of the potential risk posed to and through online social research.

To meet objective 3) Document and analyse current legislation and regulations which are relevant to social research on/ or via the Internet and assess their potential impact on current research guidance and practice, the data I investigate comprise legislation and regulations of cyberspace (see appendix 1). Chapter five focuses on privacy policies and terms of service; and on three bodies of legislation: data protection legislation, children's legislation and surveillance. These data were chosen as they represent the key ways in which cyberspace is shaped that are of direct relevance to our online social research practice. They are directly relevant because they set out how we are allowed to interact with

each other in cyberspace and how this is enforced. I produced a research schedule that amongst other things examined how legislation and regulations define cyberspace and the Internet; how they impact on social interaction; and whether they address online social research. This information is important as it is not something that is usually considered by the field and has only relatively recently come to be recognised.

My work, therefore, can function as a basis that informs other research. Reviewing the legislation and regulation of the Internet and cyberspace that is of relevance to online social research is significant. It is significant in that it provides evidence that there is a need to do so, informs of the relevant legislation and regulation, shows ways in which social research is impacted upon, and demonstrates that there is a need to include legal and regulatory matters into our methodological and ethical guidance of online social research. Deciphering how these elements shape cyberspace and interactions within it allows me to then analyse current guidance and practice to make judgements on how successful in managing arising potential risk the latter are. This is important as it can inform the development of updated legal-ethical guidance for online social research.

To meet objective 4) Critically evaluate ethical guidance in the context of the emerging legal and regulatory Internet and cyberspace to ascertain how suited they are to managing risk in online social research, the data I use in chapter six consist of a sample of ethics guides and codes of practice (see appendix 2). These were chosen because I consider them to be the most influential guidelines.

They are the most influential codes because they are discussed or mentioned by key authors, or they are from the home institutions of Internet researchers, professional associations, government and key international bodies. I produced a research schedule of key themes that examined how these guides define the research environment; what the ethical issues are, and how they are to be solved; what the legal issues are and what legislation is applicable; and whether they claim newness and difference between online and offline research environments. Furthermore, guidance targeted at online research is compared and contrasted with that which is targeted at offline research. The emerging key themes are then assessed in light of findings of the previous chapters particularly the law and regulation chapters four and five. By reviewing current ethical guidance, comparing and contrasting online and offline guides, and assessing their ability to resolve legal and regulatory issues, I generate evidence that allows me to clarify whether there is a need to update current guidance and indicate the areas which are in particular need of addressing.

In Chapter seven I review the overall findings of my research bringing together the sociological conceptualisations of cyberspace with legal and regulatory conceptualisations, and in light of findings of chapters five and six offer a judgement call on in how far current ethical frameworks of social research are able to manage potential risks that arise out of this online research environment or through our research activities. I conclude by offering a possible implementation plan of the consequences of my findings.

The original contribution of this thesis and its methodology to the field is that it is one of the first pieces of work that brings together many different aspects of how social research engages with 'new' research environments, resulting social research ethical frameworks and connecting these with legislation and regulation to reflect on online social research's ethical guidance ability to manage perceived and real risks. This is important because the Internet and cyberspace are chiefly created through legislation, regulation and their code as they frame social interaction via the Internet in cyberspace- something previously disregarded by social science. This then has a direct impact on social research practice. Thus this thesis offers a basis from which to formulate informed legal-ethical online social research practice.

1.5 Delimitations

In presenting a piece of research it is important to be, and to make the reader, aware of the possible limitations of the conducted study. In order to make the project manageable and to ensure depth of argument the study focuses on the social sciences such as sociology, anthropology, criminology, while also drawing on media-communications studies, and social psychology. This broad focus on many disciplines may appear to make the above claim of focus ludicrous; however, the focus is firmly on those disciplines' shared research principles and methodological and ethical approaches with regards to online social research. One of the early findings of my research is that the issue that I am addressing applies across all fields of social research and beyond online social research.

Hence, taking the approach of selectively identifying relevant factors across several fields makes this work applicable beyond its actual target.

Another delimitation is that the study did not consult with potential research participants of online research on their views on research ethics and practice. This means that my approach may be accused of being paternalistic. However, the purpose of this thesis is to engage with the current methodological basis of and the actual guidance provided to social researchers to assess to what extent they manage potential risk in the online environment, rather than to produce new guidance, which I argue would necessitate the inclusion of the views of potential research subjects. I have been aware of this issue and have attempted to counter its effect, by drawing on findings of previous research that informs on the attitudes of research subjects to online social research, while analysing the ethics guides and laws and regulations of my sample.

Further to this the thesis is based on the legislation and regulation that existed at the time of study 2003 - 2010. While I have made efforts to keep it up-to-date the examples within the thesis may become outdated relatively quickly as existing legislation and regulation may be repealed and new legislation and regulation may be introduced. I have therefore focused the arguments presented in this thesis on the underlying issues that are brought about by, rather than on specific, legislation and regulation. However, one has to accept that future legislation and regulation may radically change the Internet and cyberspace, which is why I argue for the

need of a continuous review of the legislation and regulation that informs online social research guidance.

One final restriction of the study is that it is couched within Western discourse on the Internet and cyberspace. With the Internet being an almost global network and cyberspace an almost global phenomenon, there are countless understandings of, meanings ascribed to, activities permitted, activities prohibited, and cultural practices assigned to them. These are not only culturally distinct but also differ along other factors such as lifestyle choices, ideology and economic activity. The issue here is, for example, laws that are made to address issues in cyberspace are informed by a socially and historically situated understanding of the Internet and cyberspace. This means that these laws create and legislate a culturally specific space, and to do justice to all of them lies outside of what is achievable within the context of this study. However, this thesis is not about identifying the cultural contexts in which cyberspace is created, or why certain laws have been put into place. The thesis examines the potential impact that these laws have on online social research.

Furthermore, the thesis focuses on those laws and regulations that an English speaking online social researcher is most likely to encounter. Consequently, there may be Internet legislation of some countries that is not included in my analysis. Yet, reflections within this thesis offer Western researchers a basis from which to formulate informed legal-ethical online social research practice.

Chapter 2:

Social science encountering cyberspace

2.0 Witnessing the birth of a new social research field?

In chapter one it emerged that social research ethics are under pressure from a variety of factors such as pluralism, ambiguity, globalisation, changes in communication tools and means of movement, shifting and competing legal and regulatory frameworks and a postmodern morality. These factors conspire to potentially turn every kind of social research into risky research. First reflections on my initial research project suggest that online social research is particularly affected by this. The senior academics at my PhD progress panel, but also beyond them others in the literature, disagreed on how they conceptualised the Internet and cyberspace and thus their resulting positions on:

- its appropriateness as a research environment and tool
- the ability of current ethics guidance to manage the risk therein
- the level of tension between ethics and legislation/regulation

Thus, this chapter outlines the key debates that conceptualise the Internet and cyberspace as a research environment and tool and thereby begins to outline how social researchers themselves assess the ability of current social research ethics guidance to manage the perceived potential risks of online social research. To begin with I locate the literature and the key debates within it. I then consider claims of newness and difference of online research tools before moving on to

discuss claims of the impact that these new and different tools have on methods and ethics of social research.

2.1 Locating the debates

After the initial search of this area the overall picture that emerged was one of three separate bodies of literature. These can be categorised into: 'Traditional' social research methodology vs. online social research methodology; 'traditional' social research ethics vs. online social research ethics; and 'traditional' social research law vs. online social research law. In the following sections I engage with these bodies of literature in order to locate the debates and examine their inherent key claims while all the while reflecting on what we can learn about social research's approach to this particular research environment, particularly with regards to managing risk.

Several general observations on online social research methodology writing can be made. Hine (2004) tells us in a review that online research publications are ever increasing in numbers from 1995 onwards, spiking in 2002, and stabilising since then. The most influential writing on online research methods is published in readers. The readers and books most referred to by the authors whose work I have read for this thesis are: Johns et al. (2004), Batinic et al. (2002), Hewson et al. (2004), Best and Krueger (2004), and Ó Dochartaigh (2002). The next most commonly referenced publications are specific research methodology books followed by a large number of articles in journals, online journals and on websites.

Key examples here are: Mann and Stewart (2000), Hine (2000; 2005), and Sue and Ritter (2007).

The writing comes in several forms. Textbook Readers (e.g. Buchanan, 2004) tend to offer a wide range of methodological discussions by authors drawing on their personal experiences, writing reflexive accounts on their decision making and particular research projects. This kind of publication serves primarily as a tool of reflection on social online research and has the secondary purpose of guiding future research activity of less experienced colleagues. One often finds attempts at methodological guidelines as conclusions of chapters which are nearly always put forward somewhat hesitantly (Ess, 2004).

Then there are books and articles on specific methods where the author attempts a more general tour de force on a particular methodological issue or particular method of online social research. These publications can be understood as an attempt at establishing a research framework that is similar to that of previous research methodologies and methods. I refer the reader to the work of Hine (2000) 'Virtual Ethnography'. This book does not just examine virtual ethnography; it attempts to contextualise it to give it a raison d'être. The author invests a considerable amount of time in discussing time, space and technology to create a space for this new and different way of research. She argues successfully, however, that in order to accept that virtual ethnography is new or different the reader has to accept the existence of a new and different virtual space.

Another way of writing about online social research comes in the guise of what I would call practical handbooks/ texts. These are less concerned with conceptualising the field and more focused on 'teaching' the reader how to actually do online social research practically. One may find guides on website design, email questionnaire designs or uses of online research packages in these texts. An excellent example of this is Sue and Ritter's (2007) book 'Conducting Online Surveys'. The authors present a compelling argument that current debates on online surveys are not that different from the debates of surveys via telephone or mail, only to insist that "the idiosyncrasies of online surveys with respect to planning, development, distribution, and analysis of the results warrant detailed attention"(Sue and Ritter, 2007:4). Again, the reader is left with the sense that online social research is different and new.

Writing on ethics of social research and online social research ethics is even more segregated. At the time of writing I was unable to find even one mainstream textbook which covered research ethics that also addressed online social research. Also, online social research ethics texts are published in particular journals and on websites that cater specifically for those interested in mediating communication technologies. This makes information on how to manage risk in online social research difficult to access and as such potentially indirectly contributes to poor ethical practice in online social research.

Several observations can be made when reviewing the literature on online social research ethics. First, on some level, ethical considerations existed throughout.

However, ethical discussion, when present, occurs in an indirect reflexive manner and a focused discussion of the ethics of online social research is only relatively recent.

> "The problem of research ethics as applied to online environments has only recently begun to be discussed, and there is no consensus as to what recommendations should be given" (Sveningsson, 2004:54).

This missing consensus is due in part to the fact that "… cyberspace experiences that can contribute to ethical wisdom are just now developing" (Allen, 1996). A sign of this is the fact that the majority of texts do not discuss ethics per se but comment on it somewhere in the text. Hall et. all (2004) have pointed out that while there is much 'how to' information, there is almost no explicit ethical guidance on online social research. This means that the reader who is interested in ethical issues of online social research has to read between the lines to extract general points on ethical issues from very specific ethical circumstances experienced, and reflected upon, by the author. This is worthy of comment and investigation because other 'traditional' areas of research have explicit ethics texts and guidance. The 'absence' of this for online social research may be due to the relatively young age of the field; however, it may also suggest a current lack of an overall ethical agenda for, as well as a lack of, and uncertainty over, ethical guidance, for online social research.

A further observation is that writing on ethics can be described as 'learning on the job'. The manner in which ethical considerations emerge is through the research

process. For the most part, there is very little description about prior ethical considerations, or which ethical guidelines were employed. It appears that the authors chose a method, and while doing the research – particularly when things went wrong – reflected on what, and why, it went wrong in ethical terms. Reflexivity is good practice; however, this approach suggests two things: an initial lack of guidance and a haphazard way of carrying out research. To counter this imbalance periodically someone will use their online social research experience to write a reflexive account at the end of which they will offer a hesitant online social research ethics guide (Ess, 2004). I call it hesitant because authors are very clear that their guidance represents only ideas, are not compulsory, not all encompassing, and very much based on their own personal experience.

Recognising the delimitation of one's argument normally evidences good academic work; however, I suggest that this approach is also the result of the ambiguous nature of postmodern times discussed in chapter one. Consequently, it makes navigating the area very difficult for the inexperienced researcher who is looking for guidance. Beyond that when one, as in my case, comes up against the issue of legality, such vagueness in guidance becomes an obstacle to carrying out research well. Thus, while many of the guidelines could be meaningfully adopted, the way in which they are presented further re-enforces the sense that online social research ethics are problematic or at least ambiguous, and uncertain. Yet, one is also left, in no uncertain terms, that just transferring 'traditional' ethical thinking into the virtual sphere is not necessarily appropriate either.

Finally, current ethical debate in online social research is based on the law or fiduciary model of ethics (Bakardjieva et al., 2004). This model assumes that the researcher has superior knowledge and competence putting him or her firmly in charge and control of the research. There is, however, a move towards a sociological / collaborative model of ethics, with a focus on the communal aspects of research practice and reciprocity, which can be noticed in some areas of online social research debates. In evidence I offer the work by Bosnjak and Batinic (2002) who are interested in the participant beyond the point of the usual data collection. They demonstrate an awareness of the fact that research participants have an impact on research and are a researcher's partners in the research process; driven by their own motivations and needs.

When looking at the literature on social research and the law (i.e. the implications of legislation for social research activities) I suspect that much more academic thinking exists, but has not been published. I was able to detect only very little academic writing on the matter and the only group of researchers who have explicitly engaged with this question are those undertaking research with children or vulnerable respondents (Alderson, 1995).

Having reviewed the literature on online social research it became clear that one thing not addressed by the vast majority is the law. This overall lack of engagement with legal and regulatory realities of the Internet and cyberspace by social researchers can be explained in part by the literature and debates within the legal profession itself. While lawyers began to consider the Internet and

cyberspace and quickly started using the term cyberlaw relatively early on, their work was not focused until Easterbrook (1996) presented them with a real challenge. He claimed that there was no such thing as cyberlaw. In effect he asked them "why cyberlaw should not be seen as 'multidisciplinary dilettantism'" (Murray, 2007:10). In 2000 another author criticised dominant notions of cyberlaw. Sommer (2000) rejected the idea that technologies define laws. This is because "technology and law are socially mediated, bodies of law do not respect technological boundaries and technologies do not define law" (Sommer, 2000:1151). What does define laws are social phenomena in this case how we as a society perceive and experience the technology of the Internet and cyberspace.

While Murray (2007) agrees with the basic notion of laws being social constructions, he still asserts that once in a while a particular technology can impact on legal processes:

> "The technologies which are of socio-legal, as opposed to just social, effect are those that create new social challenges requiring a legal/ regulatory response" (Murray, 2007:17).

If one ignores the technological determinism that underlies his argument and adds an emphasis on uses of technologies, one can recognise how it is the ways in which the Internet may be used that shape legislation and regulation and vice versa.

Legal theorists point out though that there are considerable differences between cyberlaw and 'offline law'. This difference is given expression through the socio-

technical-legal (STL) theory. Authors identify 5 models of regulatory design: 1) public interest; 2) capture/cyclical model; 3) the economic theory; 4) the public choice theory; 5) historic institutionalism. To understand why there is a difference between socio-legal modalities of regulation in the offline and the online environment we have to differentiate them. The basis of STL theory is twofold. First, "Once one ventures into the content layer of cyberspace the environmental inertia obligated by the second law of thermodynamics no longer applies" (Murray, 2007:41). Second, this context then "permits a new flexibility in the relationship between law, society and design" (Murray, 2007:41).

Considering online social research literature, Mann and Stewart's (2000) Internet Communication and Qualitative Research book is the only textbook aimed at social scientists which actually addresses the law in a little more detail. Apart from this a few articles or chapters do mention the law – but even then only in passing. Again, this is led by those researching children as they have tried to link their writing on online social research with their previous accounts of offline social research with children (Stern, 2004). The impression that one is left with is that as long as research is methodologically and ethically sound the researcher has done his or her job well.

It may well be possible that this situation was brought about, in part, by cyberlaw theorists who "saw the potential of the Internet, and the web, to provide an independent and unregulated social sphere" (Murray, 2007:5). One explicit example of this is the following citation:

> "But in cyberspace, nothing has been done before. It is an entirely new entity … electronic communication at the moment exists almost completely outside of our legal universe" (Kramarae, 1995:15).

Combined with other ambiguities in the understanding of the Internet and cyberspace, this popular notion of lawyers may have lessened the concern with law in online social research further. However, there are those of a very different opinion. "Ethics are not our only concern but also legal matters" (Jones, 2004). Further it is argued that

> "although laws and policies developed in the context of offline research they apply to online investigations" (Olivero and Lunt, 2004:127).

Of those that do mention the law, most only apply the legislation contained within their professional ethical code of practice, or institution's code of conduct. In the UK this is normally the Data Protection Act 1998. Others go beyond this as they realise that there are more laws that need to be considered in online social research. There is the recognition that while the legal status of cyberspace remains undecided the Internet has become more and more subject to legislation. Further laws that are mentioned by authors in the UK are the Computer Misuse Act 1990, Human Rights Act Article 8, Electronic Communications Act 1986, The Children Act 1989, Copyright Act 1976. Noteworthy here is the fact that, at the time of writing, there is no discussion of recent legislation at all.

Some authors qualify to what extent law should be applied. They warn their readers that they ought not to over apply laws to research practices when considering law and online social research.

> "However, modification to research practices will depend on the legal jurisdiction under which the research falls" (Mann and Stewart, 2000:40).

One more thing to point out here is that even when authors raise the issue of law they mostly do not specify which particular act they are talking about. Instead they provide a rather general interpretation of one or even several laws (without naming them) at the same time. Often those laws are interpreted that appear to justify their actions or to criticise actions of others. One example of the latter is the following statement:

> "However, researchers who contact strangers for their survey research through email are, in essence, sending them SPAM" (Krishnamurthy, 2004:114).

This statement reflects the author's ethical interpretation. It is correct that there is EU, US and several other Nations' legislation dealing with SPAM from 2003 onwards. However, none of them address the issue of social research. They are all addressing the sending of unsolicited communication for economic or marketing purposes. Also, there are differences in what is permitted. Some laws permit the sending of SPAM as long as the sender is clearly identifiable and as long as there is an option provided to the recipient to opt out of future communications (specific Acts are analysed in chapters five and six). Thus, Krishnamurthy's statement is

actually misleading. However, as of now it is not regarded as SPAM in a legal sense when social researchers contact possible research subjects using CMC.

So far this chapter has described and begun to analyse the nature of the literature on online social research by focusing on three areas: methodology, ethics and the law. Doing so revealed that at the time of the study relatively little has been written about online social research, particularly in the areas of ethics and the law. Furthermore, there is a sense of ambiguity which is enhanced through ideas of difference and newness expressed by the segregation of traditional and online social research literature.

2.2 Claims of Newness and Difference explored

Having located the debates on online social research I now proceed to consider in detail the claims of newness and difference that social researchers make in order to establish this research environment and range of tools; and what these claims tell us about the level of perceived risk of online social research and current ethical guidance's ability to manage that risk.

2.2.1 Difference of online social research

One of the ways in which the field engages with online social research is by using the notion of difference. Difference comes in many different ways. It is evident in arguments about old vs. new technology; old vs. new research environments; virtual vs. real research environments; online vs. offline environments; embodiment vs. disembodiment; old vs. new methodologies; old vs. new

methods; and old ways vs. new ways of, for example, doing interviews. Here I offer two widely quoted examples of the innovators who are determined to create a new paradigm.

> "Doing research and collecting data online is not the same thing as offline." (Sveningsson, 2004:45)
>
> "The Internet is increasingly popular as a research site and it poses unique technological and methodological challenges." (Bakardjieva et al., 2004:338)

How these authors and followers of this position substantiate, and how others refute, their views is explored in detail throughout the following sections.

2.2.1.1 Difference through appropriation of 'new' technological tools

One of the suggested key differences is social researchers' understanding of the technology itself. Hine writes "The coming of the Internet has posed a significant challenge for our understanding of research methods" (Hine, 2005:1). Others add to this "… so the Internet is fundamentally changing the ways in which we can observe, measure and report in the human condition and societal structure" (Joinson, 2005:21). What these statements suggest is that online social research is different from other social research because of the nature of the Internet and the impact that it has on social research. However, authors who make these kinds of statements do not back them up convincingly – if at all. In many cases the authors that I have read have made these statements but not explained or defended them. If the Internet brings and requires newness and difference in

social research then it should be markedly different to other technological tools that have been appropriated by social scientists.

Joinson (2005) and Hine (2005) and others seem to take this difference in technological tools as a given. I, however, find myself in agreement with Lee who states that "the role of equipment in the social sciences has been less well studied" (Lee, 2004:869). Actually, I dare go even further and argue on the basis of my extensive literature search that, at the time of writing, only very few accounts of a particular technological social research tool and socio-historical accounts of technological research tools in general has been undertaken. There are a wide variety of short undeveloped comments provided by specific papers or general texts that use this type of material as background information. Considering the reflexive nature of contemporary social research this comes as a surprise. More importantly, it means that debates about technological social research tools tend to happen out of context, resulting in 're-inventions of the wheel', misunderstandings of the role and possibilities of particular technological developments and possibly even poor methodological, ethical and legal guidance.

One brief illustration of this are Gibbs et al. who go as far as to declare that "perhaps the earliest use of technology in qualitative research was when researchers first used tape recorders in their field studies to record interview sessions" (Gibbs et al., 2002:1). However, this is wrong and in a way represents the un-organised and divorced implementation and development of technology into the social research process. As a matter of fact sound recording was,

recognising that each technology goes through phases of popularity, the fourth technology to be implemented into qualitative social research. Before it came writing, typewriters and photography.

To investigate the question of technologically induced difference and newness I have studied the literature for information on the appropriation of technological tools by social researchers. What became evident is that at several points throughout the last century social actors have proclaimed the arrival of a new technology that was inconceivable before and that would change the world (Standage, 1999). Every time, with some delay, a few innovative social researchers, by trial and error and mostly independently of each other, appropriated the technology for their research purposes, opening up new areas of research and offering new ways of studying 'old' areas. More often than not the mainstream of social sciences has taken a long time to change its ways and apart from the tape recorder and computed quantitative analysis has not really taken up the other technological possibilities.

The appropriation and implementation of technological tools into social research over the past one hundred years has been and is driven by two key underlying reasons. One reason is the starting position of technological determinism and the other reason are methodological developments. Overall there is a desire amongst social researchers, ever since the birth of social science, to be scientific. While not necessarily true for all of social science, the problem of not being able to offer formulas of social life akin to those offered by physics and chemistry has always

troubled a considerable part of the field. It troubled the field because it put the validity and reliability of our empirical and theoretical claims into question. One of the key developments in methodological terms is the pre-occupation with scientific ideals expressed through positivist, naturalist and interpretive paradigms. The basic premise is to not influence the research subject and context in any way that would skew the research data. This is also known as the 'fly on the wall' approach. Therefore, technological tools, understood as neutral tools that control research bias, are one ideal means by which to overcome perceived key problems to produce high quality, valid and reliable social research. Furthermore, technological tools were seen as an ideal means to fulfil emerging methodological aims and objectives. However, looking at the type writer, sound recording, photography and camcorders, although they brought about advantageous ways of recording data they also brought about questions on the uses and interpretation of those data, and the relationship between the researcher and the researched.

By the early 1920s social scientists used unstructured and structured interviews in research. These were often verbatim interviews, meaning that they were reconstructed from memory, or quickly taken notes (Lee, 2004). However, this practice was soon to be thought of as unsatisfactory and unreliable. There was an increasing concern with the validity of 'from memory constructed' interview scripts. This was due to the recognition that interviewers are biased in what they ask and hear during the interview itself and when recalling the interview afterwards. Furthermore, there was frustration about the limited amount of data that the scripts provided as not every detail and event could be remembered.

Therefore researchers realised that they needed to find a means to create an instant record of the conversation to protect objectivity and to arrive at a complete record of what was said. The technology that they appropriated for that purpose was a typewriter and a stenographer.

Lee argues that it was not just the availability of new technology that the "movement from the 'interview-as-elaboration' to a more modern conception of what one might call the 'interview-as-elicitation' depended on, (…) but also on a re-conceptualisation of the interview itself" (Lee, 2004:873). In his view what was particularly important is the understanding that the interview is capable of some degree of psychological penetration. Here we can see that writing as a technology is thought to allow an improvement of the research process by avoiding bias and by enabling to meet new methodological expectations.

The implementation of sound recording is also inseparably linked to a change in methodology, particularly that of interviewing. This is what already brought about, in part, the use of typewriters and stenographers. Lee points out that "It is also plausible to suggest that the attention paid in nondirective interviewing to the utterances of the interviewee was one factor in encouraging receptivity by social scientists to sound recording as a means of capturing interview data" (Lee, 2004:876). Speer and Hutchby (2003a, b) have pointed out yet another advantage of recording, namely that it can be used to control for research bias, as it offers a more accurate and detailed account than note taking.

Reasons for the favoured use of small scale recorders stems from a naturalist desire of not influencing the research and its respondents. Similar to the reasons for using a typewriter or stenographer, the recording device was thought to be a means to capture the interview in its whole, with the added bonus of being even less detrimental to rapport than the former. This understanding resulted in social scientists of the time implementing this technology to such an extent that Lee observes critically "the tape recorder rather quickly became a 'black box' in Latour's sense of the term, a device interposed within a sequence of research operations, the inner workings and operation of which are treated in a taken-for-granted manner" (Lee, 2004:879). Thus, the tape recorder became appropriated by and incorporated in mainstream social research like no other technology before or since. Slack goes as far as to argue that "It would appear that after the invention of the tape recorder, much of Sociology took a deep sigh, sank back into the chair and decided to think very little about the potential of technology for the practical work of doing Sociology" (Slack, 1998:3).

The implementation of photography occurred for very similar reasons. Ever since Galileo "it became understood that to see through an instrument (…) was to see a more profound reality than could be observed by the eye" (Harper, 2003:183). The camera was socially constructed as an instrument that would refocus the unfocused and diverted modern view. It was thought of as impartial and allowed that people "for the first time could see the world as it really was" (Collier, 1967:3). From this point of view "Photographed images do not seem to be statements about the world so much as pieces of it, miniatures of reality that

anyone can make or acquire" (Sontag, 2003:166). Therefore, an instrument such as the camera that offered an objective means to capture reality presented a unique scientific way to study society.

One final example of how technological tools are implemented to realise methodological ideas are those visual researchers who utilise camcorders and film. The first researchers to bring together film and ethnography in the mainstream were Gregory Bateson and Margaret Mead who in their 1936-38 study of Balinese culture used not only photographs but also film for research purposes. Mead justifies the use of this technology by arguing that

> "If tape recorder, camera, or video is set up and left in place, large batches of material can be collected without the intervention of the filmmaker or ethnographer and without the continuous self-consciousness of those who are being observed" (Mead, 1995:9 cited in Banks, 2001).

Again there is a methodological desire to be a 'fly on the wall' researcher. Furthermore, epistemologically, her basic premise is that to "simply watch someone is to learn something about them, knowledge that can be later analysed and converted into intellectual capital" (Banks, 2001:112).

The research tool of the Internet is implemented for the same reasons as these other technological tools before it. It is appropriated because as a technology it is thought to be neutral and, to begin with, it is considered to be the great social equaliser and free from power and restraining factors. The tool of the Internet was attractive to social researchers because of the space that its use created, that

is full of free, equal, open-minded social actors. It also served methodological ideas of naturalistic research by making it even easier to undertake covert study; and the possibility of instant transcription further reduced costs, time and bias (Mann and Stewart, 2000). For example Illingworth writes that its use reduces "…the impact of instrumental biases such as the race or gender of the investigator" (Illingworth, 2001). In every instance the underlying reasons for the implementation of the research tool into social research offered by researchers are in line with those given for other technological research tools. The only hint at newness and difference is that some of these reasons are re-enforced by the context that the Internet – not the research tool – creates.

This sub-section re-enforces the sense that the Internet is appropriated and implemented for very similar reasons to other technological tools before it. Therefore, I suggest at this point that the Internet as a social research tool does not appear to be a new paradigm, but continues the long story of technological tools as research tools. This means that at this point in our reflections we have to assume that current ethical guidance is capable of managing the risk inherent in the use of the Internet as a research tool.

2.2.1.2 The stages of appropriation

When investigating the literature further another area of overlap and consistencies that I am able to identify are the stages in which technological tools are implemented. There are three kinds of stages that I refer to: (1) stages in terms

of technological developments; (2) stages in terms of the implementation into the mainstream; (3) stages in terms of attitudes towards the technological tool.

All the technological tools that I studied (writing, photography, film, sound recording, phones, pc software and the Internet) have been appropriated and implemented depending on the developmental state of the technology itself. To begin with when technologies first appeared only the true innovators attempted to implement them into their social research. The technological tools were often very difficult to use and cumbersome to transport and meant that many social scientists did not utilize them because of a lack of technological know-how and its impracticality.

One possible illustration of my argument is the use of film. By the early 1960s researchers began to effectively combine film and ethnography. Apart from the theoretical and methodological reasons for the implementation of this technology, the fact that synchronous sound and film equipment was now available, portable and reliable allowing filming in the remotest areas of the world was the real driving force behind its popularity. However, this equipment was expensive and needed several operators which were thought to have a negative impact on the research process, environment and participants. The fully portable video equipment changed this. It was now no longer necessary to have an entire film crew present; the camcorder was very large but could be used by one person. Thus, the practical aspect of ethnographic film was improved and it gained in popularity.

One of the pioneers of sound recording was Whitley who, in 1931, experimented with recording interviews with the ediphone, an early form of business dictating machine. However, this was unsuccessful as it had poor sound quality, was not easily transported and involved the continuous and difficult changing of the recording tubes. Further to this sound recording remained on the fringes of social sciences due to the costly technology, transcription costs and time, and the need for main levels voltage, even though the latter was solved by the introduction of batteries. Technologically, the past two decades witnessed the leap from cassette to CD then mini disc and finally to digital recording devices. These technological improvements made sound recording much easier, cheaper and efficient; thereby, arguably, leading to a rise in the number of social researchers utilizing these technological tools for their research purposes.

The use of the Internet as a research tool has developed along technological innovations. To begin with most research focused on text-based interaction, this meant that it was not considered of value by some. Chen and Hinton, referring to Internet interviewing, write

> "As neither is able to directly see the other person, all non-verbal communication is lost and the method lacks the ability of the researcher to conduct observation based research during the course of the interview" (Chen and Hinton, 1999:4).

This is one of many more possible examples that shows that the way the Internet was implemented was clearly linked to its developmental state. Writing in 2008 one may now relativise Chen and Hinton's (1999) comments as the Internet has

added the capacity of video and voice communication that was not readily available in 1999. Similarly those studying online gaming and identity play had to rely on textual analysis (Turkle, 1996) to begin with. Now computing power means that high quality and realistic online environments have been created that allow and have encouraged a considerable growth in the number and range of studies (Guest, 2007; Taylor, 2006). Furthermore, early users of the Internet had to write their own software for research tools, something that is no longer necessary as easily customisable packages are available. This clearly shows that there is a direct link between technological developmental stage and research opportunities exists not only for previously adopted technological tool but also for the Internet.

The other kind of stages that I have identified is that technological tools are implemented into social research and its mainstream in stages. While studying the use of technological tools in social research I found that technological tools were implemented from the fringes towards the centre. There never was a move from the mainstream into specialised fringes of the field. It would generally be the innovators who implement a tool, after some delay other enthusiasts would begin to implement the tool while the centre/ mainstream of the field acted more hesitant and even critical towards the new research tool. After a while the mainstream then begins to utilize the technological tool, however, apart from a few exceptions never really fully embraces them.

An example of this is the use of computers. The first to realise the prospective benefits of this technology were health researchers. As early as 1949 researchers at Cornell University employed computers to process paper questionnaires. They found that they obtained 49% more information than a clinician would have done. Instead of being taken up by others, however, computers were not implemented by clinicians or the wider research community. It was not until 1968 that the next well documented study took place. The Mayo Clinic in the United States utilized computers for patient self-interviews. Their results were very encouraging; highly successful in obtaining data and very well received by participants (Bachman, 2003). Yet again, the research community did not pick up on this beneficial and novel research tool and consequently "the use of computer interviewing of patients is ignored in textbooks" (Bachman, 2003:67).

Quantitative researchers were quicker to appropriate the mathematical and thus statistical potencies of the technology to help with their data analysis. Important to remember is that this was only from the late 1960s onwards. Qualitative researchers took the first tender steps into a new way of dealing with their research data only in the 1980s. Even then, Weitzman and Miles argue that "the only programs most people had heard of were those that carried out quantitative content analysis of text" (Weitzman and Miles, 1995:4). This is not surprising considering that the majority of qualitative research books made little if any mention of the probable application of computers (Weitzman, 2003). But this changed slowly between the early to mid-1980s, when there was a growing interest in the possible application of existing word processors and data base

programs. The early programs specifically designed for qualitative research purposes were not developed by professional programmers but by qualitative researchers themselves and thus ended up being awkward and difficult to use. These early versions focused on data management, but the ways of possible application were expanded on quickly (Weitzman and Miles, 1995; Gibbs et al., 2002).

When investigating the Internet as a research tool one can also recognize the stages of implementation found with other research tools. The Internet has been used as a research tool for over 20 years now albeit in the mainstream only in the last couple of years. What is interesting to note is that with this technological research tool it appears to be students from within the mainstream that are arguably the driving force behind its implementation. Evidence for this is the increasing number of students who use the Internet for all or parts of their research projects. The professionals of the mainstream, however, appear to be more hesitant, yet there is growing acceptance of this 'new' research tool. In evidence for this I would offer attempts by Bryman (2004) to include guidance on Internet research in his mainstream research methods text book, the increase in the number of courses on the Internet and cyberspace, and an increasing number of projects using the Internet being funded by the ESRC. However, as all the other technological tools, apart from the Dictaphone, the Internet has not been fully embraced by the mainstream for the collection of primary data, yet.

The final stages that are to be discussed are the stages of attitudes towards a technological tool that can be identified. As within a wider societal context and outlined above the attitudes towards technological tools undergo changes. In general there is a move from uncritical to critical attitudes towards technology. This occurs in two ways. Firstly, towards technology in general but also towards and 'within' particular technologies. By this I mean that in general people, including, social scientists, have embraced technology unreservedly as a force for positive change and later on grown more critical as the dark side of technologies became seen. After analysing the use of technological research tools I add to this that each technological tool undergoes its own cycle of this. To begin with innovators and their followers think of the technology as the ultimate tool to warrant 'perfect' valid and reliable social research. Later on, however, there appears to be a shift away from this unquestioning implementation to a more critical and realistic engagement with the technology. Most of this occurs in line with a wider societal shift in attitudes towards technology post World War II. However, this reflexive engagement with technology is present in social research long before this too. I offer the detailed example of photography to illustrate this point.

Similarly to the technology of writing, the camera was implemented unreservedly into the social research process. The prevalent position of the time was that of objectivism and utopian-futurism. From this position technology was viewed as a neutral and from human desires unaffected thing, that when used in social science would make findings objective and more scientific. However, continuing the

exploration of photography, in the second half of the 20th century social scientists started to take a different theoretical position. The camera was deconstructed and reconstructed as a technology that was, contrary to previous thought, deeply influenced and shaped by its user. It has become accepted that the camera is highly sensitive to the attitudes of its user and "a tool of extreme selectivity" (Collier, 1967:4).

The, at the time, ubiquitous theoretical perspective of social determinism rejected the naïve position of objectivism and meant that photographs were understood to be social constructions in two ways. Firstly, that the social positions, with regard to social power and hierarchy, of the photographer and the subject come to the fore when the picture is taken. Secondly, that the way the scene is composed reflects a tension between mirroring a socially constructed reality and the tacit imperatives of, the social constructs of taste and conscience. With this change of theoretical outlook, photographs and their analysis, produced in the early phase of this technology's use in social research, lost value. Particularly, anthropological research was now discredited which is reflected in Harper's words.

> "Anthropology was a science of the colonizer, and the images made in service of anthropology defined the native in ways that reified the relationships of superiority and inferiority endemic to colonialism" (Harper, 2003:192).

Researchers argue that it is not sufficient for contemporary visual ethnographers to just point and shoot as their anthro-colonial ancestors have done, but they

have to "become conscious of the potential to make visual statements by knowing how the camera interprets social reality" (Harper, 2003:183). This reflexive undertaking did not only concern anthropological work but all types of social research that used photographs. Sontag sums up the now prevalent attitude towards visual technology by writing

> "Although there is a sense in which the camera does indeed capture reality, not just interpret it, photographs are as much an interpretation of the world as paintings and drawings are" (Sontag, 2003:167).

Referring to photographs as paintings and drawings also indicates the 'dark side' of the camera's use in social science. The photograph itself may be changed at a later point without the knowledge of the observer. This puts into question the validity of any photograph used in social research and has led to some rejecting the employment of them. With increasing technological possibilities, particularly digital technology, the rendering or faking of photographs is, in this context, worryingly easy. There is software that can detect whether images, digital or not, have been tampered with. However, it is very expensive and not fool proof.

It is important to be aware of the fact that old photographs are not immune to being touched up. Loizos points out that

> "… many photographs of naked tribal people published in such 'realistic' photo magazines as Picture Post and Life in the 1940s had naked genitalia artificially 'clothed' or otherwise disguised, so they are misleading as historical sources" (Loizos, 2000:95).

This detailed account illuminates the shift from technological determinism to social determinism. It shows clearly how the implementation of technological research tools is affected by the overall societal understanding of and relationship to technology; and techno theoretical developments. The Internet is subject to the same changes. To some extent the Internet was pulled in two directions from very early on. While one side celebrated its freedom of speech, equality, lawlessness and the resulting opportunities, the other side felt threatened by it or at least put into question the validity and reliability of data gathered via or on it. One major difference to previous research is not the critical and resisting attitudes that Internet research has to face from the majority of social scientists; rather, it is the level of resistance that it is confronted with that is new.

As outlined earlier, all previous technological tools notably photographs and videos had been critically reconstructed when reflexivity, ethics and research governance came onto the scene. Internet research was born in the middle of a late modern, or as some would argue postmodern sociological ontology and thus was confronted right away with very restrictive research rules and attitudes. At the heart of this lie three issues. First, late modern social scientists associated technology with the dark side of progress, feeling that technology would get in between them and data and distort data. Second, a reflexive research environment meant that many researchers rejected the Internet due to ethical concerns. And third, powerful social actors, after an initial utopian embracement of the Internet for its alleged gifts of freedom and endless possibilities, became increasingly concerned with exactly that and have begun a process of taming and

controlling the Internet, by means of laws, ethical guides, public campaigns and taking active influence on Internet programming. This still does not justify, talking about a new paradigm. It appears that 'old' issues are just magnified.

This sub-section shows that the Internet is subject to the same attitudinal changes as other technological research tools. This adds further credence to my earlier assessments that the Internet as a research tool is not radically different from other technologies and therefore does not necessarily constitute riskier research.

2.2.1.3 Advantages and disadvantages of technological tools

The concluding area in the literature to be considered to assess the difference and newness of the Internet as a research tool are the advantages and disadvantages that are associated with technological research tools. When engaging with the literature it becomes apparent that the underlying advantages and disadvantages are to a large extent identical. However, interestingly, these are presented as if they were new or different to other technologies. There appears to be very little engagement with what other technologies offer in comparison or where one's chosen technological tool fits in. The only comparison that is really drawn is that of selective traditional methods. So for example one may draw upon the example of how the tape recorder is better than pen and paper, but not how it relates to other technologies. Also, the disadvantages of technological tools are mostly divorced from the fact that these disadvantages are not new, but have already been present for previous research methods where they were either thought of as

negligible problems or resolved satisfactorily. To illustrate these assertions I draw out key examples that are of particular relevance to Internet research.

Some of the advantages of the Internet directly address concerns first raised with the technology of writing and methodological issues of bias, limited data, and interviewer effects. While the Internet as a research tool may offer advantageous solutions, the key point is to recognise that the issues are the same and that the Internet is used as a tool to fulfil methodological ideals that have been around for 100 years.

When reviewing the issues around film in social research, it appears that there is another parallel to Internet research. Both technologies initially were thought to have a detrimental effect on the respondents' answers and were thus used covertly at times. They both also witnessed a shift in opinion and are now considered to not have a detrimental effect after all. There are some similar ethical issues that arise for both, namely that of consent. The question being: How does one receive informed consent from all individuals?

There are other parallels to sound recording too. One of the major advantages of sound recording as mentioned above is that of providing a complete and un-biased audio record of the interaction. The same can be the case in Internet research through the use of communication tools such as messengers (e.g. Skype) and freely available recording software.

There are those who view Internet research more critically. Some of the criticisms are along the lines of being concerned with issues such as computer literacy of researcher and respondent, establishing contact, ensuring cooperation, loosing access and interactive online skills (Mann and Stewart, 2000). These are very much in the same vain as the concerns voiced with telephone research. Another similarity is that both technologies are thought to have either positive or negative effects on social interaction and self-identity. Also, Internet, just like telephone researchers, have to take the reasons for their respondents' participation into account, which is not the case with other technological tools. This is because there is the disadvantage that there is no face-to-face interaction between researchers and subjects. This is thought to lead to a lack in rapport which makes recruitment difficult and the validity and reliability of data questionable. Interestingly, this is all carried out with complete ignorance of other tools that have this problem. One example is postal questionnaires. Bosnjak and Batinic's (2002) research into motivations for participation in Internet research when compared to motivations to participate in phone studies shows that the reasons for participation are identical. Another criticism that Internet research shares with that of computer assisted analysis is that it is too far away from the data and the respondent.

So far Internet research represents very much a continuation of the appropriation of technology into the social research process described in this chapter. It is more than a continuation; it embodies the convergence of all the other previous

technological research tools into one multi-media medium. This suggests that Internet research is practically speaking not a new paradigm. But is that so?

While engaging with the literature on Internet research and taking the evidence provided in this chapter thus far into account, it is impossible to miss that there is one key difference between other technological research tools and the Internet. This difference is cyberspace. In the literature on other technological tools there is no sense whatsoever that the researcher or the user are leaving their physical location. Nonetheless, in Internet research this is exactly what happens. This is because some propose that "Computers create digital domains: parallel universes where events occur outside the usual physical spatial constraints" (Chesher, 1997:79). More specific to the Internet it can be pointed out that "The language and imagery used to describe and promote computers refer to new spaces…" (Chesher, 1997:80). It is surprising then that connecting computers via telephone lines changes everything. Nunes brings this to our attention by writing

> "One does not 'go' somewhere when picking up the telephone. But when the computer couples with these same telephone lines, suddenly spatial and kinetic metaphors begin to proliferate" (Nunes, 1997:166).

Consequently, using the Internet, a researcher enters a new space of social interaction, travelling into the world that is within the phone wires, located between the telephones/ computers.

Extending this understanding leads us invariably to the following statement:

"The Internet has become a non-physical space where many people interact across countries and national borders, social class and gender …" (Holge-Hazelton, 2002).

This has been widely accepted for quite some time and means that the technological research tool of the Internet is practically no different to other technological tools other than in one crucial way. It apparently removes the researcher and his subjects from the real world and moves them into a parallel virtual world called cyberspace. Therefore, I suggest that the question of whether we need new legal-ethical guidance for Internet research can be answered with no. However, recognising that the Internet is the tool and cyberspace is where we use it we have to further investigate whether this 'new' and 'different' space poses new risks and whether current ethical guidance may be able to manage these new emerging risks.

The purpose of this sub section was to establish whether the research tool of the Internet differs sufficiently from previously appropriated technological tools that it presents its own paradigm and thus requires new ethical guidance in order to manage the risks that its use may create.

The key findings are that:

- The starting point is that of technological determinism for the appropriation and implementation of technology into social research.
- The second key reason for the implementation of technological tools are methodological developments.

- Technological tools appear to be implemented independently of each other.
- The mainstream is slow in the uptake of technological tools and at times even hostile to it.
- The appropriation and implementation of technological tools follows stages, most notably from unreserved implementation to reflexive/ critical engagement.
- There is considerable overlap on the advantages and disadvantages of technological tools presented to us. Yet there is no recognition that this is so as discourse is couched in 'newness' and 'difference'.
- The above points are all true for the technological tool of the Internet.
- Drawing on the concept of convergence the Internet can be understood as the convergence of several previous technological research tools not just in terms of technology but also in terms of social research methodologies, practices, advantages and disadvantages.

At this point I would be able to argue that current social research ethical guidance can manage risk in online social research as the Internet as a practical research tool is not different enough as to create risk that current guidance cannot resolve. In order to assess this latter point, however, I need to investigate the ethical impact that using these converged tools bring about. To this end I continue my investigation by critically engaging with the claims made by social researchers on the impact of this research tool on the methodological and especially ethical framework.

2.2.2 Newness of the research field

As mentioned above in section 2.1, writing on online social research methods and ethics tends to be based on a personal account of research experience and is often couched in claims of newness and difference that researchers make. These claims of 'newness' come in two forms: First, that their particular article, chapter or book is the first one to address the issue at hand in detail. Second, that online research as a whole is new. One thing the keen observer notices is that for reasons of need to prove originality, and staking a claim on the 'new' field of research, the majority of enthusiasts' accounts claim to be the first ever, the most detailed and the 'newest' on the topic. Here are some prime examples of how authors are positioning not only themselves but also the field as new and different.

> "… discussion of email as an academic research tool has, to date, been scarce." (Selwyn and Robson, 1998:2)
>
> "While there have been some early initiatives in a qualitative research setting, there has been little systematic analysis of how the Internet might be incorporated into qualitative research practice." (Mann and Stewart, 2000:4)

The second form of newness is the claim that online social research is a new field of social research with new methodologies and methods. Here I provide several quotes to illustrate this point.

> "Online survey research is still in its infancy." (Sue and Ritter, 2007:3)

> "… it is necessary to develop a new set of research skills which address the challenges which the Internet presents." (Ó Dochartaigh, 2002:6)

> "The hyper-linked, co-produced and evolving characteristics of the web necessitates reconsideration of traditional research methods, and the development of new ones." (Schneider and Foot, 2005:157)

> "As society transforms and is transformed by new technology, so there are new ways in which qualitative researchers collect and analyse data and new forms of data to collect." (Gibbs, Friese and Mangabeira, 2002)

> "Among these interviewers there was a general consensus that, in order to interrogate computer communication, a new research methodology was required." (Mann and Stewart, 2000:5)

Those focusing on ethics argue in a similar vein. Siang (1999) writes that it is difficult to apply previous ethics codes to online social research because of the distinct features of the virtual self. Examples of these distinct features that the author and others provide include: the blurred distinction between public and private domains, the ease of anonymity and pseudonymity, the transcending of spatial barriers, communities of dispersed members, suspension of temporal barriers, archiving and recording possibilities and low-cost means of tracking participants, ease of data collection (Siang, 1999; Kleinman,2004).

Others add to this by claiming that the traditional ethics codes stem from a time before late-modern forms of communication. "The Internet, simply put, poses issues, problems, and concerns that were not anticipated when regulations were established" (Lee, 2004:109). Furthermore, there are times when traditional guidance "… does not reflect the reality of current Web research practice" (Porr and Ployhart, 2004:115).

Bober comments that

> "using online methods raises particular ethical issues, and so far researchers conducting virtual studies have relied mostly on moral values as ethical rules on how to obtain data from online respondents are only just emerging and far from consistent" (Bober, 2004:290).

The above arguments are the basis from which many researchers argue that there is a need for adapted if not even entirely new ethics codes for online social research. All of these authors reveal their beliefs clearly. They believe in the existence of a parallel world that is different in that it offers new ways of social interactions and thus new and different social research opportunities.

Consequently, they argue that there is a need for new research methodologies and ethics. At this point I do not deconstruct their argument –which I undertake later on in chapter three– but use their statements to draw out some insights into what a possible answer to my research question may include. If there is a cyberspace and if it is as different and new an environment as suggested then this

would suggest that social research has to review in particular what kind of risks emerge out of this space and whether current ethical guidance can manage these.

By 2004 this consensus was widespread and influential throughout the literature in this area. Some authors clearly felt frustrated and even let down by traditional research methods expressing

> "…traditional qualitative research methods have failed to keep pace with technological advancements in online environments." (Johns, Chen and Hall, 2004:2).

Therefore,

> "the arrival of electronic media requires a redefinition of what constitutes legitimate research and acceptable methodology" (Johns, Hall and Crowell, 2004:119).

At this point, if I were to rely on this argument I may answer my research question and the dilemma in the initial research project by stating that current ethical guidance cannot manage risk adequately and thus there is a need for new ethical guidance because cyberspace is a new and different environment requiring new and different research methodologies and ethics. It is the fact that the field has not kept up with modern communication technologies that has made my initial research project's methodology vulnerable. This, however, would be a polemic and self-indulgent position to take and furthermore be not informed by the wider arguments in the field.

Online research sceptics argue that either the application of 'old/ traditional' methods in this 'new' environment; or the new methods are too problematic. Alternatively, they question the quality of social interaction in cyberspace and thus the quality of research possible. The most extreme scepticism is that there is no new social environment and thus there cannot be such a thing as online social research. An eloquent representation of this position is the opinion of Janowski and van Selm who state

> "… much more is to be gained through application of conventional research methodologies and practice than those who are on the vanguard of the Internet research innovation seem willing to acknowledge" (Janowski and van Selm, 2005:200).

The arguments by Schneider and Foot (2005) and others are put into question by the members of this camp. Chen and Hinton write "… method is an application of an existing technique rather than a wholly new research approach" (Chen and Hinton, 1999:2). Their views are supported by Johns, Chen and Hall (2004).

> "Online social research moulds traditional qualitative research methods to the Internet environment. (…) It folds virtual and real-world inquiry into the same set of interpretive practices" (Johns, Chen and Hall, 2004:1).

Interestingly, these views do acknowledge the difference and newness in environment (virtual-real); nonetheless they do not attempt to create a modernist dichotomy (online vs. offline research) but to distinguish between practical differences and ontological and epistemological continuities. Cyberspace exists,

but social interaction still continues, maybe in different ways, nevertheless informed by the same socio-cultural realities.

Adding further evidence to this, various commentators argue that while some online social research methods are still in their early phase of development and the technological tools are new, the methodological issues put forward by proponents of the need for newness are not (Sue and Ritter, 2007). They do so by taking a list of the known online social research methodological issues and comparing it to the list of methodological issues facing 'traditional' social research. From their point of view the underlying issues are the same.

These authors are joined by those who do not share the sense of need for adapted or new ethics (Jones, 2004; Peden and Flashinski 2004). Jones even regrets the timing of the discussions on online social research ethics as they "… are taking place at a time when research ethics are becoming increasingly confused and mixed up" (Jones, 2004:44). Furthermore, this author feels that online social research has been singled out unfairly for 'special treatment' in a way no other type of research has (Jones, 2004).

More disinclined to and outspoken about the idea of new ethics is Thomas (2004). This author identifies a different reason other than newness and difference for the current ethical debates.

> "Organizational self-interest and liability concerns become translated into ethical discourse, and the ethical discourse becomes translated into the

rhetoric of self-interest – based on policy formulation legislation and enforcement" (Thomas, 2004:196).

While some may consider this overly polemic, Reips (2000) provides Thomas (2004) with the evidence that allows him to raise the issue and thus, inadvertently, supplies another reason why online social research is 'different and new'. It is because

> "… the high visibility of (overt) Internet research and its increased public availability opens online research to evaluation by a wider audience – including potential participants. To this extent, there is added impetus to comply with standards – and be seen to comply with them" (Denscombe, 2005).

To summarise the opposition to the idea of new ethics for online social research I offer the following citation.

> "I argue that we need not invent new ethical rules for online research or try to reduce ethical behaviour in Internet research – or any other- to an immutable set of prescriptions and proscriptions. We need only increase our awareness of and commitment to established ethical principles" (Thomas, 2004:187).

The ethical issues that authors have outlined which arise in online social research include: informed consent, traceability and confidentiality, invasion of privacy, reporting of findings, researcher- participant relationship, recruitment of participants, traceability of subjects, rejection of and hostility to the researcher,

over-researching, SPAM, data collection (cookies, etc.), and making previously invisible social interactions visible.

At this point one is tempted to agree with Thomas' statement that "[t]he fundamental ethical questions posed by new technology are not new" (2004:198). However, maybe these issues are not new in the ethical sense but in the technical sense. Denscombe hints at this while writing on online surveys:

> "Ethical standards are especially important in online surveys, due to new (often) technical issues concerning privacy, data security and sampling" (Denscombe, 2005).

As an illustration, briefly consider the example of researching under age subjects online. Stern argues that "…implementing youth research in online environments raises significant ethical issues" (Stern, 2004:274). The author argues that these issues differ from offline ones. When inspecting the issues outlined – parental consent, ethical responsibility of the researcher – on the surface, one could refute calling them new or different from offline issues. Considering the technological realities, however, a different understanding emerges. Particularly the matter of parental consent appears in a new light.

Re-calling Denscombe's (2005) idea that ethical issues are new not so much in a purely philosophical but in a technical sense helps understand issues that social scientists face in online social research. It also unmasks some declarations on the newness of ethical issues as overstated. More importantly, it adds another level to ethical considerations. This means that one may not only need new ethical

guidance when there are entirely new ethical issues associated with a particular research tool. One needs new ethical guidance when the technical aspects of that tool impact on previous ethical issues rendering them into new forms also.

Some issues that are thought to be unique to online social research are traceability, netiquette, SPAM, privacy invasion. Williams and Robson tell us that

> "…Witmer, Coleman and Katzman (1999) found a hostile response from several of those canvassed. Many of those contacted objected to receiving 'junk mail', while in William's study (2003) several respondents were concerned with the infringement of privacy resulting in many of the responses demanding to know how the researcher obtained their email address" (Williams and Robson, 2004:30).

Nonetheless, under closer examination those issues are not new. It is correct that users can be traced more easily than previously in traditional forms of research, however, the basic ethical considerations involved are identical.

Netiquette is another example of researchers over-estimating newness and difference. First and foremost most online researchers are not aware of or ignore netiquette in their discussions. There are a few, however, who correctly point out its importance.

> "It is important not to breach netiquette whilst undertaking research as the result will be few responses and a barrage of mail informing a researcher of their non-compliance" (Coomber, 1997:13).

Therefore, the researcher

> "must take account of both codes of conduct relating to behaviour in computer-mediated communities, and concerns the codes of conduct relating to the practice of social research" (Williams and Robson, 2004:40).

This is not a new issue. Whenever a researcher enters any field he/she has to abide by the etiquette of the particular context, or research subjects will suffer the consequences.

Considering Spam, Kaczmirek and Schulze write "Spam is unethical communication practice from the standpoint of consumers for six reasons – privacy violation, volume, irrelevance, deceptiveness, message offensive and targeting vulnerable consumers" (Kaczmirek and Schulze, 2005:115). I argue that they raise important matters for consideration. However, these considerations are only new in that they are played out through use of different technological tools such as emails or Instant Messaging Services (IMS). The underlying ethical considerations are not new and play as much part in traditional mail survey research.

Nevertheless two things are different/ new. First, users' knowledge of using Internet tools is higher than in other research contexts. This is because there is a much smaller competence gap in Internet research than in other traditional forms of social research. Subjects have more insight which potentially makes them more critical (Bakardjieva et al., 2004). Second, the technological tools involved mean that it is very easy and convenient to give feedback- much more so than previously.

The only ethical issue that comes up that is arguably unique to online social research is that of over-researching a particular group. It may well be possible that this could happen with traditional research tools too, however, the chances of this are remote. The issue of over-researching emerged after there was a large increase in the number of online research projects (Williams and Robson, 2004). This resulted in particular groups, often vulnerable ones, being studied over and over again, mostly without their knowledge or consent. They would learn about the research by finding their communications published online and/ or offline. This way of research, however, is increasingly considered an infringement on their personal space and rights to privacy. As a response researchers are often told in no uncertain terms that their research activities are not of interest to or welcome by the potential sample. Further, more and more groups post a clear statement in their terms of use documents on online social research making it clear that they do not want to be subject to research activities.

Trying to make sense of this some write

> "We find this kind of aversion to Internet research highly disturbing and suspect that the current narrow notion of research ethics, with its indifference to fostering subjects' interests and goals, has something to do with it" (Bakardjieva et al., 2004:345).

This means that online social research does potentially raise ethical issues that previously were not pertinent, and thus supports calls for not only a re-examination of traditional ethics but the creation of new ethical guidelines in order

to manage this 'new' risk. We can use Illingworth's work which focuses on methodology in general to shed more light on this. He writes:

> "While the methodological difficulties are similar to those experienced in the more conventional research domain, they are more acute within this field." (Illingworth, 2001:6)

His claim appears to rest on two givens: 1) issues are not the same but similar; 2) the matter of amplification. The examination of the arguments around ethical issues illustrates that Illingworth may to some extent be correct. However, at this point, just because the methodological issues are more acute does not mean that current ethical principles cannot manage risk in online social research and thus we need 'new' methodologies and ethics. It means that we need to work through our methodological and ethical considerations more thoroughly. But if the underlying issues are the same then that does not require 'new' guidance or methodologies. Newness in this case is about updating methodologies and guidance, not about identifying new ethical issues and finding ways of resolving them.

This latter point is re-enforced by this statement:

> "We seem to feel the need to speak of virtual focus groups, online ethnography, cyber-research and web experiments to distinguish old familiar methods from their new offspring" (Hine, 2005:5).

In this case difference and newness is called upon semantically to distinguish different variations of traditional methods being facilitated by new means. It may be seen as a criticism of this approach and questions the merit of a call for new

methodologies and ethics. However, I believe that Hine's point is more subtle than that. While she is trying to frame enthusiasts' claims, her work is representative of the third camp of 'appeasement'.

The supporters of the third position of 'appeasement' strive for a compromise between the arguments outlined by the first two positions. Their ideas are informed by notions of the Internet extending existing social environments rather than creating separate ones. They also talk of mixing online and offline methodologies to contextualise research.

Attempting to offer an intermediate position Kendall writes:

> "Ethnographers of online spaces confront many of the same problems as researchers practicing more traditional ethnographic methods, as well as some new ones" (Kendall, 2004:125).

Here the author does not suggest a complete difference between old and new, but hints at the addition of some new ones.

Overall this sub-section shows that depending on the philosophical stance that one chooses, one views online social research methodology and methods either as entirely new; old applied in new social environments or old yet magnifying issues. On the whole this situation means that

> "…there is considerable anxiety about just how far existing tried and tested research methods are appropriate for technologically mediated interactions" (Hine, 2005:1).

It also means that we have to re-examine our understanding of research methodology and what methodologies entail before and while doing online social research.

2.3 Transferable ethics

The realisation of the applicability of the Internet and cyberspace as a research tool for social research has brought about a sharp increase in social research being carried out via or in cyberspace. These activities have caused some debate within mainstream social research in general and within online social research in particular about its merit, and brought about disagreement and uncertainty about the applicability of 'tried and tested' traditional methodology, and ethics in this 'new' research environment. There is no clearly defined framework for harmonizing the different positions. Further, the impact of the legislation and regulation of the Internet and cyberspace is not taken into account by the majority of online social scientists and has only recently (January 2008) become a more consolidated project within the specialised field as evidenced in the new journal publication of the International Journal of Internet Research Ethics.

The basis of debates on online social research is newness and difference or some level of refutation of such claims. Difference is important in that the new environments cause different social interactions, different ways and means of identity formation, and different means of engaging in social research or not (quite). Newness in that authors consider online social research occurring in a new environment with different factors affecting social interaction causing new

ethical issues to arise or not (quite). Thus there is the possibility of current ethical guidance not being able to manage the new risks that may emerge in this new research environment and/ or tools. Thus there may be a need for differing/ new methodological and ethical considerations and ethics codes and ethical practice or not (quite).

At this point the overall impression is that current ethical guidance is adequate in managing risk of online social research tools. The review of debates in the literature shows that what changes this, however, is the fact that most social scientists accept that the use of the Internet is considered to create a new sphere of social interaction called cyberspace. The research tool of the Internet then becomes the means by which to access and carry out social research in this new social environment. The term online social research is suggestive of a considerable contextual 'newness' and 'difference'. Thus while the technological research tool – the Internet – is not 'new' and 'different' when compared to previously appropriated technologies, the fact that its research occurs via or in this new social sphere demands further inquiry into the question of whether current ethical guidance is adequate in managing risk in online social research. There is a shift of focus. It is no longer about the tool itself but the research environment – cyberspace – which has to be engaged with in order to answer my research question. Therefore, chapter 3 considers different conceptualisations of this 'new' and 'different' research environment while assessing in how far they warrant the need of new ethical guidance for online social research in order to manage this new spaces' inherent risks.

Chapter 3:

Mapping a new frontier

3.0 Ontologies of cyberspace

Chapter two located the debates in the social science research literature re the topic of online social research with a particular focus on online methods, ethics and the law. While investigating the practical research tools and the resulting positions on how successful current ethical frameworks are in managing the perceived risk of these tools it transpired that the tools themselves are not actually as new and different as some suggest but rather signify a convergence of past tools and one may argue a magnification of already known ethical dilemmas.

Throughout the chapter, however, the literature discussed hinted at an underlying matter that requires our further consideration. This matter is the fact that the use of the converged tools either create or at least offer access to a new realm of social interaction – cyberspace. Many , if not all, of the claims of newness and difference of online research tools are deeply rooted in the believe that there is a cyberspace that is considerably different from offline social environments and thus puts into question the usefulness of current ethics frameworks of social research. This chapter considers how the Internet and cyberspace are conceptualised to investigate in how far a new context emerges in which offline morality and thus current ethical guidance is not able to manage risk in online social research.

3.1 Difference between the tools and the spaces

Throughout the thesis I am using the terms of the Internet and cyberspace almost always in immediate proximity to each other. This may give the impression that they are the same, and indeed some may use the two terms interchangeably. I do not use them interchangeably, however, as they represent two interlinked concepts. The Internet is the technological communication tools that through their use by social actors arguably grant access to cyberspace. Thus at the beginning of this chapter I outline our current understanding of the Internet before proceeding to discuss the dominant and often competing ontologies of cyberspace.

> "The Internet is arguably the most significant development in communications to emerge in the past century, carrying a promise to revolutionize workplace, education, politics and leisure pursuits" (Atkin, 2002:25).

Drawing on the works of Abate (2002), Lin (2002), Atkin (2002) and Kitchin (1998) I am able to provide a brief summary of key developments of the Internet. The birthplace of the Internet are the United States of America. In the 1960s, after the Russians had built and successfully launched Sputnik, the US military was given the task to develop a network that was secure from nuclear attacks. The basic intent, expressed very simplistically here, was to create a network that while some sections may be disconnected still allowed for the passing on of information.

By the mid-1970s the governments of Canada, Germany, Norway and Sweden were running their own networks and were beginning to be connected up with each other. The 1980s witnessed a remarkable expansion of the Internet; however, user-friendly applications were missing. At this point the interaction was text based, search engines were non-existent, and the only real activities were that of email and file transfer. From the 1990s onward new technological developments turned the Internet into what its users know it as today. Two researchers at the research institution CERN programmed the World Wide Web Internet application (www). This created the basis for further technological convergence and development creating the foundation for websites, blogs, webcam and voice messaging, discussion forums and chatrooms and other social media such as Facebook, Twitter and YouTube. All of this made the networks user-friendly, thus changing the perception of the Internet from being a research tool to possessing new roles, uses and meanings for entertainment, shopping, self-presentation, and social interaction.

3.2 Stepping through the screen into cyberspace

In the following sections I study the ways in which fictional accounts and political actors have shaped our understanding of our online social interactions and experiences in cyberspace and thus our understanding of cyberspace itself.

3.2.1 Charting the birth and the cultural dispersal of cyberspace

This section considers the birthplace of the concept of cyberspace and its spread throughout Western culture to become a common sense understanding of what

happens when we use Internet technologies. I consider there to be a range of contexts of reflection which cross fertilise each other's ideas. These are literature, media and powerful social actor's engagements with the topic.

Cyberpunk fiction has been identified as the birthplace of the concept of cyberspace. It is often argued that cyberpunk fiction is postmodern fiction (McCaffery, 1991). It is the response to late/ postmodern desires to reflect on the social and scientific issues in contemporary society. I begin this charting with cyberpunk not only because it is the birthplace of the term cyberspace but because it: Firstly, recognises and understands the socio-spatial process that underlies the late-modern condition; secondly, offers informed visions of possible futures; thirdly, provides cognitive spaces in which to think about contemporary society; and fourthly, inspired readers to attempt the realisation of its visions in contemporary society (Dodge and Kitchin, 2001). As I will show later on in this chapter, while it may be easy to dismiss cyberpunk as simple fiction, it has had a dramatic effect on how other popular culture mediums, the media, powerful social actors and even social researchers have conceptualised the Internet and cyberspace. This in turn then will have an impact on how we understand the morality of cyberspace and thus the kind of risk that it poses in online social research and current ethical guidance's ability to manage said risk.

Inherent in cyberpunk fiction is the social and political constructivist conceptualisation of technology and society. Frank Knarf offers the following summary of the genre:

> "Cyberpunk literature, in general, deals with marginalized people in technologically-enhanced cultural 'systems'. In cyberpunk stories' settings, there is usually a 'system' which dominates the lives of most 'ordinary' people… . These systems are enhanced by certain technologies, particularly 'information technology', making the system better at keeping those within it, inside it. Often this technological system extends into its human 'components' as well, via brain implants, …. Humans themselves become part of 'the Machine'" (alt.cyberpunk).

In the early 1980s Gibson, walking past an arcade, noticed how children were 'hooked' to the machines playing games. Later on, while reflecting on this impression in a series of articles, he coined the word that has since come to symbolise one of the ages of man, cyberspace. The term entered the social consciousness in 1984 with the publication of 'Neuromancer'. In it Gibson offers the first definition of cyberspace:

> "[Cyberspace] … a consensual hallucination … A graphic representation of data abstracted from the bank of every computer in the human system. Unthinkable complexity. Lines of light arranged in the non-space of the mind, clusters and constellations of data. Like city lights receding" (Gibson, 1984:51).

Users hook themselves into their computer and leave their bodies behind when entering cyberspace. A space populated by others, full of opportunity but also danger.

In his story "Burning Chrome" (1986) individuals use a device called cyberdeck that affects their sensory perception and doing so enters them into cyberspace. Soon after the publication of Neuromancer (1984), many other writers from within the genre of cyberpunk applied Gibson's idea of cyberspace to explore social issues and phenomena in a futuristic setting.

In 1995 fantasy writer Williams turned his attention to cyberspace and wrote the Otherland series. In his story, characters have to hook up to interfaces that allow them to enter cyberspace. There is an element of digital divide in his novels, as only the rich can afford interfaces that allow a truly real experience. In his account cyberspace, referred to as Otherland, is this beautiful alternative space that consists of multiple parallel worlds, all with their own rules and realities that have passages that connect them to each other. He presents a darker side of it as he writes about the potential abuse of cyberspace by the powerful.

One of the key themes when defining cyberspace that emerges in cyberpunk writing is that of the distinction between real life (RL) and virtual reality (VR). The first refers to individuals' physical, mortal, geographical location. The latter refers to the individuals' multiple, pseudo physical and dislocated from RL geography, mostly immortal cyberspace presence. Interestingly, on the surface it appears to reflect a modernist dualism – the real vs. the unreal, natural vs. unnatural. Even the characters in the stories express this quite clearly as the following excerpt shows.

" 'What blew up?' He chewed rapidly. 'People killed?'

'No one, thank God.' She tried not to be disheartened by his clear look of disappointment. 'But it destroyed the campanile – you remember, the tower in the middle of the campus.'

'Chizz major! Who did it? Zulu Mamaba?'

'No one knows. But it frightened me.'

'A bomb went off in my school last week.'

'What? You never said a word about that!'

He grimaced in disgust, then wiped grease from his chin. 'Not that kind. In SchoolNet. Sabotage. Someone said that some guys from Upper Form did it as a graduation prank.'

'You are talking about a system crash on the net.' She wondered for a moment if Stephen understood the difference between the net and real life." (Williams, 1996:33)

There is a clear distinction between real and virtual. However, for some it seems this distinction is being steadily diluted and possibly begins to disappear. Due to its late modern outlook this is where science-fiction ends and cyberpunk begins. Modern distinctions fall away with the rise of the hyperreal.

"…the clarity and depth and immediacy of the Vertex are so fantastic that my body believes, in some dimension both shallower and deeper than logic, it is actually standing in New York in 1850." (Foy, 1996:38)

"Now, when you say 'Is this a real place?' you are asking a very difficult question. An apple is a real thing, yes? But a picture of an apple is not an apple. It looks like an apple. It makes you think about apples, you can

> even choose one pictured apple over another in terms of which might taste better – but you can't taste either of them. … It's only a symbol, no matter how realistic-looking, for a real thing. … But if you could touch it, and it was wet – if you could drink it, and quench your thirst – then would it not be water? It is hard to imagine something that is real and not real." (Williams, 1996:38)

The hyperreal is almost complete when cyberspace experiences can no longer be distinguished from offline experiences. The hyperreal becomes real when as in the "Otherland" narrative by Williams characters whose online avatar is killed, die offline too. Dodge and Kitchin sum this up by writing "Every space within which we reside becomes an intermediate blend of real and virtual. Modernist notions of neutral, objective, measurable space thus dissolves as the systems of knowledge which support such notions collapse. Here, space, in human geographic terms, is meaningful only as spatiality: produced, contested and ephemeral" (Dodge and Kitchin, 2001:191). Therefore, the distinction between real and virtual is only useful when describing the context of social interaction, not to describe two parallel worlds.

Fictional writing on cyberspace is not only the preserve of cyberpunk though and its basic premise was also adopted by other genres to further reflect on the relationship between society and current emerging and converging technologies of the Internet. One example of an author exploring cyberspace in less of a technological futurist way is Sinha. In her book 'The Cybergypsies' (1999) she

tells the readers of the risks of overdoing it online and its almost dramatic effects on offline identity and personal relationships. Interestingly her writing removes itself from the well-trodden path of the 'going online' into cyberspace that one is accustomed to in cyberpunk stories and alludes the reader to a far more complex reality of computer mediated communication (CMC).

Throughout she allows us insights into her character's inner thoughts and uses them to tell the reader about her conceptualisation of cyberspace. To her, cyberspace is about social interaction via phone lines and computers and pages on screens, which at the same time create a sense of presence that is almost absurd to the rational onlooker, yet real to the user. The following are some excerpts of one paragraph that I have broken up to explicate her argument.

> "…Mister Slutfucker vanishes from the screen to delve in the hidden part of his bulletin board, the grandly named Oklahoma Institute of Virus Research. It isn't a 'real' place. It has no existence in space-time" (Sinha, 1999:5).

> "It is a computer-generated mirage, a cloud castle, a Fata Morgana, yet real people meet here and start things which ricochet into the real world" (Sinha, 1999:5).

> "Geno's board is a piece of software that lets my computer, via modem, call his. Once past the electronic portcullis, identity and password verified, I'm genuinely inside his system, or the bits of which he allows me to see" (Sinha, 1999:5).

What emerges from these excerpts is that it is not very difficult to distinguish between real and virtual. There appears, as first to be a clear understanding that cyberspace is not a real place, it does not exist in space nor time. This suggests that it does not exist at all. At the same time cyberspace is described as a mere Fata Morgana. But, they certainly do exist in space and time. Thus, somewhat confusingly, this fantasy space that is not real has very real effects on real life. In the last quotation the author clearly identifies the problem with assessing what cyberspace is. She writes that it is the technology that communicates through signals; however, suddenly the character is genuinely inside another user's system – suggesting presence.

From this writing the cyberspace that emerges is based on users communicating with each other via technological means that somehow create a space with many places in it that is not real, yet can have real effects on real life.

Another indication that cyberspace is becoming part of Western daily experience and the concept by which we understand the impact of its reality is the 2006 publication of 'Cyber Cinderella' by Christine Hopkins. In this story a young woman is dissatisfied with her life and decides to Google her name on the Internet only to find a website dedicated to her by a secret admirer. However, life that she supposedly lives according to the website does not match her own interpretation of her life as the cyberspace version is a lot more exciting. The quest of finding that admirer makes her live so much more like the life described on the website

that she begins to wonder what is more real, the person Izobel Brannigan or Izobel Branningan.com.

Again to begin with the story tells us of a dichotomy – real vs. virtual. The physical world is real and cyberspace is the other place where we can dream about who we could be. In this case the author goes one step further allowing a stranger to narrate the main character's life story. Thus cyberspace is a place where we can lose control over our identity. Then, however, at some point, cyberspace and reality penetrate each other, with the result that Izobel loses her sense of what is real. Cyberspace is yet again another sphere of social interaction that, while separate from the real, can impact on it. This separateness is elusive, however, and the dichotomy of the two worlds appears to break down once a 'critical mass' is reached, putting into question our knowledge of the world – the ever present modern dualism.

While these examples exhibit how adult cultural artefacts engage with the relationship between modern communication technologies and society I offer one further example, children's literature. I do so because children and young people are growing up with these technologies and associated narratives around them and thus arguably experience these technologies as a 'natural' part of their social world referring to the cultural narratives available to them to make sense of this. This is relevant to our overall understanding of cyberspace as their understanding of the space will shape their interactions in it and thus determine whether current

ethical frameworks can manage risk of online social research in the emerging morality of cyberspace.

Coleman wrote a series of children's adventure books (Netbandits, 1997; Cyberfeud, 1998) in the mid to late 1990s that were based on activities on the Internet and in cyberspace. In his stories he depicts cyberspace as a sphere of information. He really does make clear efforts to avoid cyberpunk narrative. Instead he focuses on the use of computer mediate communication (CMC) between techno-savvy children and their 'contacts' and friends and the information available online to solve crimes in the real world. Cyberspace emerges as an information and communications network. Metaphors of going online, surfing the net, on the net are present in the texts, but are not intended to infer earlier cyberpunk imagery and conceptualisations of cyberspace.

An entirely different approach, far more in line with traditional cyberpunk, is offered by Richard Peck. His book 'Lost in Cyberspace' (1995) creates this cyberspace that allows cellular reorganisation – meaning that the characters can fax themselves through cyberspace and by this means travel through time. Cyberspace appears as a time machine then. His second book 'The Dream Machine' (1996) takes the idea of a genie in a bottle and substitutes the bottle and the genie with cyberspace. Through computer programming a cyberspace is created that grants wishes. Compared to other conceptualisations of cyberspace Pecks version is much more 'playful'. Nevertheless, it holds true to the utopian vision of cyberspace creating parallel worlds that can be journeyed through,

altering time, doing away with geography, that have a real impact on real life and that also hold dangers.

At this point it is possible to delineate the dominant literary imagery of cyberspace. Cyberspace is a sphere of social interaction that to begin with appeared to be a parallel world to that of the real world. It was considered a virtual world. To enter this virtual world, users had to employ technologies. They cross the threshold into this 'other' world by turning themselves into a cyborg, meaning physically connecting their cerebral bodies with a machine and thus blurring the modernist dichotomy of humans and technology.

Upon stepping through the gateway, users could then move around this 'new' parallel world, their movements only limited by their own imagination or the spatial design rules put into place by the powerful. Cyberspace is a space that is split into public and private spaces. It reflects the late modern notions of public space being eroded by private spaces- through private company or individual ownership. Cyberspace mostly replicated offline/real spaces, values, norms, identity roles, and relationships. As technology became more sophisticated the distinction between the two worlds; real vs. virtual began to be undermined. The rise of the hyperreal was completed with the first user killed online, dying offline. Thus cyberspace is the space where the signifying has become as good and real as the signified; and thus has moved from the late modern to the postmodern.

Interestingly there is a tension in the literature between the cyber-fictional accounts and the fictional accounts. The former defines cyberspace as outlined above, however, the latter reflect the contemporary cultural struggle of making sense of cyberspace. Novels by Sinha (1999) and Hopkins (2006) clearly recognise the fact that cyberspace's uses permeate the social fabric, however, they struggle explicating what cyberspace is. They move back and forth between cyberspace as parallel world; cyberspace as an extension of the social world; and cyberspace as a huge computer network. This tension can be explained by the ontological positions of modernity and postmodernity that these accounts draw on. What we are left with is the strong sense that cyberspace is a parallel world that ultimately does away with our understanding of real and unreal or real and virtual, leaving modernist dualism behind.

These representations in cyberpunk and more main stream fiction will have affected how some in society understand cyberspace directly; their real impact was only permeated indirectly via the medium of film and news media that as the following sections show have heavily relied on them. These in tern then affected powerful social actors who draw on these ultimately cyberpunk narratives to explicate cyberspace and to exert cultural control over it.

Another fictional genre that took the idea of cyberspace to a much larger audience is movies. Over the past 23 years the movie industry has used technological advancements to visualise cyberspace for the masses. No longer was it confined to the images conjured up in readers' minds by words, now people could see it

with their own eyes. Arguably the film that started the age of cyber films was Tron (1982). This is now regarded a classic and was the first movie to be computer generated. In the story a computer programmer's body is turned into molecules and sucked into his computer. He encounters a parallel three dimensional world where programs are represented as people with feelings and a will of their own, living in a dictatorship under the MCP (Mast Control Program). The visual narrative tells of a world – cyberspace- and life in this virtual world is as, if not worse than, in the real world. There is no direct contact between these two worlds and movement between them is limited to humans going in and humans coming out. Still, events in the virtual world impact on the real world.

Then, probably mainly due to commercial reasons – seeing that the first couple of cyber films failed at the box office- the next 13 years did not produce any notable cyber films. From the mid-1990s onwards, however, the public was repeatedly confronted with visual narratives of cyberspace. This is possibly explained by two factors. Firstly, the massive spread of personal computing and Internet access, making it more relevant to social beings to be provided with means to reflect upon their experiences. Secondly, advances in computer graphics and special effects enabled film makers to represent cyberspace visually in entirely new ways.

Johnny Mnemonic (1995) is a full-length motion picture that is based on Gibson's short story and also incorporates elements of other Gibson books such as Neuromancer (1984) and Virtual Light (1993). Drawing on the cyberpunk images the movie tells the viewer about a world that is connected by a huge Internet.

The real world is threatened by a dangerous disease and can only be saved by the main character, who as a cyborg carries the information about the cure on a chip in his brain as cyberspace is too insecure to transmit the information in.

This narrative of cyberspace is of interest because it not only tells the viewer about cyberspace but also about the real world and how the two are linked. Cyberspace is a huge network, a space of lawlessness and danger, where no-one can be trusted. The real world is a postmodern world where humans have become cyborgs – part human part machine that is also full of danger. Humans can be used as physical emails in order to bypass the Internet. Nonetheless or because of this, cyberspace and the real world have permeated each other.

The Net (1995) is of interest because it, just like Sinha's story, places cyberspace into a contemporary context away from the purely fictional. The film describes a world where virtually everything is done virtually. It is a world of information with endless opportunity due to the global network known as the Internet. The film also depicts the net as a place where shy 'cyber-jockeys' meet and spend their nights chatting. The main character is shown as aware of her sheltered and somewhat lonely existence but is happy with it. However, the safe existence that she enjoyed in cyberspace turns out to be the source that will bring turmoil and mortal danger to her real life.

The world of 'The Net' is a place that has become 'fluid'; fluid because the truth can be manipulated as it does no longer exist in physical evidence but numbers.

This is expressed by the fact that the main character is 'deleted' by a hacker. Identity is about the information that exists on you in cyberspace, if that is altered you change, if it is deleted you no longer exist. Again, cyberspace – the virtual world- has permeated the real world. It has not replaced it, but has become so much part of it that actions within this social sphere of interaction affect all other spheres- even the physical ones.

The Matrix (1999) took cyberpunk to an entirely new level. Not only did it offer incredible visualisations of cyberspace it also brought it to a huge audience, influencing popular ideas of cyberspace around the world. It is also revolutionary because it attempts a Galilean coup de grass by stating that our real world/ life is a computer simulation and that 'we' are really in cyberspace. Real life is virtual and the true real life is spent lying in a vile gel being used by technological beings as batteries for their colonies. It is arguably a truly postmodern narrative that is heavily influences by relativism not only questioning all Western understandings of space, place, identity and reality but obliterating them. Cyberspace is no longer fiction but is not real either – the real no longer exists. Nonetheless, the physical real makes a modernist return by characters choosing – or not- the vile lying in the gel reality over the computer simulation. The human nature comes through to fight the technology to safe humanity. Thus, in the end cyberspace is unreal, very convincing yet still only ever virtual, a parallel world that is accessed and left through turning a human into a cyborg to encounter a world that is based on what we conceive as real, that can hurt and kill, but still is only a signifier.

The movie 'You've got mail' (1998) does not naturally come to mind when thinking about cyberspace. It is worth considering because it was viewed by an audience that would not normally be classified as a science-fiction audience and may arguably have had a wider reach than most of the other movies discussed. In the story the two main characters meet online in a chat room and send each other emails. In real life (RL) they do not get on at all, yet in cyberspace, they tell each other of their private truths, and fall in love. The message is that people are more honest in cyberspace, as they control the information about their identity and due to anonymity do not have to wear everyday masks nor cater to their RL social role expectations. While appearing to present a positive narrative of cyberspace, the movie also makes it clear that it can ever only be a substitute and is only secondary to RL relationships, physical appearances and social roles.

In review, the birthplace of cyberspace lies in cyberpunk and it has been further appropriated by other genres such as fiction, movies and games to not only tell compelling stories but more importantly to reflect on contemporary experiences of technology in general and mediating communication technologies in particular. Interestingly, even though authors of those narratives seldom acknowledge their sources of stimuli, reading their texts as a sociologist, one can easily identify a whole range of contemporary social issues and social theories.

The majority of conceptualisations of cyberspace marry the 'techno-centric' with the 'socio-centric'. They draw unashamedly on ideas of utopian futurism and technological determinism while describing the space from a social constructivist,

Marxist and feminist perspective. This is why computer mediated communication technologies can create a space of social interaction, that is kept alive through social interaction, that frees users from their flesh while utterly corrupting their minds and potentially killing their offline identity and even body. It is a rather postmodern space that rather than following industrial revolution's and other technologies' gradual move from utopian to dystopian ideas, has, if at all, undertaken this journey in the instance of its conception. Cyberspace, as conceived by fiction, is the Wild West of the 21st century, full of opportunity yet marred by danger. Added to this is a late modern tendency to favour relativism. Thus, cyberspace is a mix of real vs. virtual, and disembodied vs. body.

While the cyberpunk literature purely fictional and philosophical in its conceptualisation of cyberspace, novels and movies have begun a process of moulding it in a way that allows the application of the idea of cyberspace to address contemporary experiences of technologically-mediated communication and notions of risk and future risks and social phenomena and possible societies.

While there are slight deviations, the overall understanding of cyberspace that can be arrived at is that it is a space created through technology, where users can interact, that has the potential to liberate, but as in the offline world is laden with power relationships. The sense is that a potential tool for overcoming Weber's salvation anxiety has been wasted and thus cyberspace is nothing more but a reflection and extension of the real and the ugly that is society.

3.2.2 Popular conceptualisation of cyberspace

In the following section I investigate how key definers in society understand cyberspace and its experience of their use of computer-mediating technologies; and what are the resulting public accounts of cyberspace all the while showing how they relate to the above fictional accounts.

3.2.2.1 Powerful public social actors

Nine years after his initial use of the term cyberspace, Gibson stated in an interview that cyberspace is the space where telephone calls take place. Furthermore, people were navigating cyberspace –the realm in which geography no longer exists- when they used the Internet (josefsson.net, 1994). Interestingly, Gibson proposes two things.

Firstly, he attempts to change our understanding of 'where' telephone calls take place. There was no notion amongst telephone users of going anywhere – their conversations were situated in their respective physical localities and only their voice was projected via a technological medium. Now, Gibson pulls telephone calls away from the locations of the users and puts them somewhere in between into a different space - cyberspace.

Secondly, he suggests that this space becomes unlimited three dimensional space when users access it via the Internet. Thus he reinforces his earlier ideas about the existence of an alternative space of social interaction that is similar and yet infinitely different to 'real' space by rooting it in our common past. By this I mean

that by utilising the telephone as a portal into cyberspace, Gibson appears to suggest that cyberspace has been with us for over 140 years and allows him to connect his fictional creation –cyberspace- with reality. It is no longer part of a future depicted in cyberpunk narrative, but is real, and has been for a long time. The use of the computer and the Internet are only better vehicles to travel within it.

Gibson's conceptualisations –fictional as well as in RL- of cyberspace impacted on public opinion makers and technologists. "Many utopian analysts and politicians have drawn on Gibson's writing in formulating their own visions of the future and to justify investment in information and communications technologies" (Dodge and Kitchin, 2001:186). Interestingly, while encouraging exactly this by his statements, Gibson views the ways in which his work is influential, critically. In an interview he stated

> "I was delighted when scientists and corporate technicians started to read me, but soon I realized that all the critical pessimistic left-wing stuff just goes over their heads. The social and political naïveté of modern corporate boffins is frightening, they read me and just take bits, all the cute technology, and miss about fifteen levels of irony" (Gibson, 1989:59).

What Gibson expresses is his frustration that educated people are still stuck in modernist ways of thinking about the world; they are reading his work as fiction that is about to become real, not as postmodern cyberpunk that warns of 'blind' technological development.

One of the most influential cyberspace prophets is Barlow. He is acknowledged to be the first public figure to apply Gibson's cyberspace ideas to the technological phenomenon of the Internet and computer mediated communication (CMC). Barlow, a self-styled cybernaut of the new realm, writes:

> "Today another frontier yawns before us, far more fog-obscured and inscrutable in its opportunities than the Yukon. It consists not of unmapped physical space in which to assert one's ambitious body, but unmappable, infinitely expansible cerebral space. Cyberspace. And we are all going to go there whether we want to or not" (Barlow cited in Chesher, 1997:82).

He goes further, arguing that cyberspace heralds:

> "the promise of a new social space, global and anti-sovereign, within which anybody, anywhere can express to the rest of humanity whatever he or she believes without fear. … Our identities have no bodies, so, unlike you, we cannot obtain order by coercion" (Barlow cited in Loader, 1997:4-5).

Barlow and Gibson are critical in the analysis of conceptualisations of cyberspace because they have provided not only the terminology but also linked fiction and reality. Most importantly, they offered a tangible framework to Western society for understanding and acting in a 'new' sphere of social interaction that is created by social actors through their uses of communication technologies.

Drawing on the ideas of this section so far it is possible to delineate that cyberspace is a space of social interaction that is unlimited in size; free from

government regulation; equal; bodiless; and a cerebral space that lies outside of the real world.

Barlow, however, did not only consider himself a cybernaut but the defender of the new realm. Consequently, he and a couple of other cyberspace utopians, founded the Electronic Frontier Foundation (EFF), which has popularised the term 'cyberspace' even further. It sees cyberspace as "a Jeffersonian frontier, peopled by many small freeholders all with equal rights" (Gozzi, 1994:220). This is also reflected by their 'Blue Ribbon' campaign where they argue in favour of freedom of speech in cyberspace.

There are now many more cyberspace interest groups and organisations on local, national and international levels, all adding socio-cultural narratives of cyberspace. They can be government organisations, semi-public organisations, private organisations, and industry organisations. These organisations have different purposes and outlooks depending on the group's conceptualisation of cyberspace. The organisations can be split into two camps; firstly into those that consider cyberspace in need of regulation, and secondly, those that want to protect cyberspace from (too much) regulation. One example of a group wanting regulation of cyberspace is that of the American Bar Association. In 2000 they published a two year report warning of the threat of global chaos due to the Internet and cyberspace. Thus they demanded flexible cyber-borders and a global commission overseeing cyberspace (Heise Online, 2000). On the other end of the scale we find groups such as Privacy International. Founded in the UK they

describe themselves as "a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations" (Privacy International, 2006).

The apparent dichotomy exists only in their response to and not the underlying definition of cyberspace. Both camps agree that cyberspace is another social sphere that is distinct from the physical/offline social sphere that offers freedom from real life socio-cultural and legal constraints. What is also interesting to point out is that cyberspace is not a static concept or phenomenon. Cyberspace is defined by these organisations as much through their mission statements as through the impact their actions have on the social interactions and thus the spaces of cyberspace.

One instance of this is the effect that the Cyberspace Research Unit (CRU) has had on Western –particularly British- understandings of cyberspace and the way it was subsequently designed. The unit is working on cyber security of children and implicitly defines cyberspace as a sphere of social interaction that due to its lawlessness, easy access, anonymity, and potential for criminal abuse is a source of dangers to children and vulnerable people. Therefore, cyberspace is in great need of regulation. They subsequently published reports and programmes such as the 'Cyber Stalking, Abusive Cyber Sex and online Grooming: a programme of education for teenagers' (2004). This document, amongst others, builds the basis of Msn and other Internet service providers' way of designing services for their underage customers. Consequently, this example illustrates how organisations'

understanding of cyberspace and their resulting actions shape the visual representation, the type of communication enabled, the 'feel' of cyberspace - the reality of cyberspace. This does not only apply to groups that pursue regulation but also to those resisting regulation as both starting positions through subsequent action result in a particular appearance and thus conceptualisation of cyberspace.

Another group that actively constructs cyberspace are politicians and governments. Here again one is able to identify a common understanding that is obviously based on Gibsonian and Barlowian notions of cyberspace, while at the same time two opposing reactions emerge. I begin by discussing the positive at times utopian arguments. Former US Vice-President Al Gore announced in a speech:

> "One helpful way is to think of the national information structure as a network of highways, much like the interstates of the 1950s. These are highways carrying information rather than people or goods" (Gore cited in Chesher, 1997:83).

The former Speaker of the House Newt Gingrich also subscribes to this version of cyberspace as for him it is the land of knowledge and the "exploration of the land can be civilization's truest, highest calling" (Gingrich cited in Elmer-DeWitt, 1995:8).

To illustrate the dystopian accounts of cyberspace I focus on two themes: cybercrime and paedophilia, and cyber-terrorism. Of interest at this point are

political statements only, this is to derive the political conceptualisation of cyberspace. The important legal conceptualisations that have emerged out of a desire/need for regulating cyberspace and their impact on Western understanding and the actual form of cyberspace will be discussed in section 5.3.

3.2.2.2 Cybercrime and paedophilia

Relatively early on governments and businesses realised that in order for the economy to use the Internet and to make profits, cyberspace had to be a safe environment. A lot of the debates were about whether the government should be the regulator or whether the government should regulate the cyberspace companies into self-regulation. One example is the letter written by the Chief Inspector of the Metropolitan Police to over 140 UK Internet Service Providers (ISPs) in 1996.

> "This list [of pornographic news groups] is only the starting point, and we hope with cooperation and assistance of the industry...to be moving quickly towards the eradication of this type of newsgroup from the Internet. We trust that with your cooperation and self-regulation, it will not be necessary for us to move to an enforcement policy." (Metropolitan Police Service, 1996, cited in Anderson, 1998:23)

Again cyberspace is imagined and presented as a separate lawless social sphere that offers great benefits as long as it is properly regulated. In the UK the government had taken and still does take a laissez faire attitude and does only

intervene into cyberspace regulation when absolutely necessary. There are other countries such as the US or Germany who take a more active role.

Former German Home Secretary Schily during a G8 meeting on "Security and Trust in Cyberspace" (2000) demanded a strong international regulation of cyberspace. Expressing what many of his colleagues felt - that cybercrime had become a threat to public security and the information society. The conference ended with a strong sense that cyberspace must not remain a lawless space. The way forward was international legal consent and clearly defined laws.

Interestingly the original prevalent 'love' for the Internet and cyberspace for all its freedom and progress, that heavily relied on a technological determinist outlook, was quickly replaced by worries about the negative effect communication technologies and especially social interactions found in cyberspace could have. Some political statements appear to suggest that cyberspace had turned from heaven to hell. Instead of the home of the civilised human being striving for knowledge and global human interaction (see Gingrich), the great equalising force had become home to cyber thugs, identity theft, rape, fraud, conspiracy, and hackers.

I argue that the debate that changed Western understanding of cyberspace forever is that of online paedophilia. Drawing on Cohen's (2002) and Butler and Drakeford's (2005) theories on moral panics and scandals suggests that the moral panic and scandal surrounding online paedophilia is – at least so far- the moral

panic of the 21st century. Not only does this case tell us about the dominant ideological conceptualisation of cyberspace in Western culture but also shows how actions executed on these definitions reshape cyberspace into a different phenomenon.

One example is the closing down of first MSN chat rooms and later on Yahoo! chat rooms due to a moral panic about paedophiles lurking in dark corners of cyberspace. Another example are training courses offered to children and to parents by interest groups such as NSPCC, teaching the safe navigation of cyberspace.

All this constructs a narrative about cyberspace that is akin to the Brother Grimm's 'Little Red Riding Hood' or 'Hansel and Gretel'. Cyberspace is this dark forest that is part of this world, and yet does not bow to its laws, with dark dangerous creatures lurking, waiting to get you – and they can even get you in your own or grandmother's house! This place has to be tamed by a warden –i.e. governments, the police, Internet Service Providers (ISPs), and interest groups. Therefore, while cyberspace is still dark and dangerous there is light at the end of the tunnel prophesying a safe and orderly parallel social world sometime in the near future.

3.2.2.3 Cyber-terrorism

A search of the 2005-6 cyberspace literature reveals a massive shift in focus over the past couple of years. Using US American lingo, 9/11 changed everything. Beginning with the publication 'Black Ice' by Verton in 2003 cyberspace discourse

has become centred around the threat of cyber-terrorism. The book, while of little academic value in itself, nonetheless offers deep insights into the political and governmental conceptualisation of cyberspace from the 1990s and especially since 9/11 from and American perspective.

The issue of cyber-terrorism is not that new. The Clinton administration ran defence exercises in cyberspace and released the first 'National Plan' to defend cyberspace in January 2000 (Verton, 2003). What is new, however, is that while during the Clinton years cyberspace was predominantly defined in positive and – some argue utopian or naïve ways- since 9/11 2001 US politicians and government have deconstructed that positive understanding of cyberspace. Access to information and education are considered cornerstones of a modern democracy. Therefore, cyberspace was thought so highly of, because it offered an unprecedented stream of information and education. However, what was thought of as a strength became now part of its overall dark side.

[Al-Qaeda]

> "was using the Internet to do at least reconnaissance of American utilities and American facilities. If you put all the unclassified information together, sometimes it adds up to something that ought to be classified" (Clarke, former chairman of President's Critical Infrastructure Board, 2002)

The new conceptualisation of cyberspace came into effect when President Bush announced, on the signing of the Homeland Security Act 2002, that:

> "…the department will gather and focus all our efforts to face the challenge of cyber-terrorism, …" (President Bush, 2002:2127)

This speech along with other similar commentary stated in US policy reconstructed cyberspace as a territory that is the non-physical extension of the US without clearly marked and protectable borders, making the country vulnerable to terrorist and foreign attacks. The response, naturally, is to compensate for this by an aggressive policy of regulation –taming the wild expanse before them, bringing law and order; just as their forefathers did when they journeyed west. The political and governmental unease about cyberspace stems from the fact that it has now formed the backbone of the economy and all other central infrastructure services such as electricity, gas, water, and oil.

Other Western countries have responded in very similar ways. However, there are some politicians who call for a middle way. They warn of defining cyberspace as a 'Wild West' that needs to be fiercely fought over and strictly controlled; instead they suggest an alternative understanding and approach.

> "We must also reject the false choice of liberty versus security. We can and must have both." (Ridge, former Director of Homeland Security, 2001)

By arguing this Ridge returns to what former German Foreign Secretary Fischer meant when he warned in 2000 of the overregulation of cyberspace and called for a balance between individual freedom and protecting the security of the state.

Using what is said about cyber-terrorism to gain insights into the political conceptualisation of cyberspace reveals a space that is something like the fourth border. By this I mean that a country's traditional borders are ground, sea, and air; now there is a new one- cyberspace. There is, however, still uncertainty about where this cyberspace border lies as some of it just like the national waters off a coast, still belongs to a country. What is certain is that beyond it lies a huge lawless expanse – no man's land that is too big as it grants potentially uncontrolled/able space that can be the source of danger. What is important for understanding political conceptualisations of cyberspace is that it has moved from defining cyberspace by its virtues as a free, liberal space of social interaction to defining it by its potential dangers.

So far this chapter has discussed the birthplace of the concept of cyberspace and then moved on to discuss how it was spread via cultural media and powerful social actors into the dominant element underpinning our understanding of cyberspace. When reflecting on what these conceptualisations of cyberspace tell us about morality and risk, I arrive at the opinion that cyberspace is a space where adhering to moral frameworks is particularly important as it is an extension of the social world into a new sphere of social interaction without some or even any of the norms, regulations and legislation of the offline world. The potential of offline spaces for good and bad is considerably magnified in the online environment. At this point the above 'data' does not tell us whether this brings about new ethical dilemmas or whether 'old' ones are just amplified. However, even amplification

may mean that current ethical guidelines may not be able to adequately manage risk in online social research. Of concern is also the contradiction that cyberspace is described as lawless and under-regulated when in fact the above examples of legislative, regulatory and policing activities tell of a far less free space than used to justify its further taming. Whether there is an actual lack of legal taming is secondary as it nonetheless leads to ambiguity out of which may arise risks that current ethical guidance cannot manage.

To gain a deeper insight into this I now move on to uncover the ways in which social scientists have attempted to conceptualise cyberspace in order to establish whether current ethical frameworks are able to manage risk in online social research.

3.3 Academic conceptualisations of cyberspace

The academic conceptualisations presented in this chapter are drawn from a wide range of fields including sociology, social and cultural anthropology, psychology, communication studies, technology, criminology, and gaming theory. While many of these fields lie outside of what would normally be considered sociological inquiry they are to be included to reflect the multi-disciplinary approach to cyberspace and to counter the unawareness of each other's work amongst sub-disciplines.

To clarify, the aforementioned professions, now more so than in the past, are combining their talents in a multitude of possible combinations to study

cyberspace; however, that was and is not always the case and as online research is carried out on the fringes –by highly specialised sub-groups- of mainstream subjects, many findings are not shared. This makes an inclusive approach such as offered by this chapter important. It is important because it allows this thesis to offer a transdisciplinary foundation from which to make its arguments and it permits future inquiry to benefit from a multi-dimensional understanding of cyberspace. This strengthens theoretical and empirical research by making researchers more reflective of their own practices, preventing the 're-invention of the wheel' and drawing on strengths of other disciplines.

The following sections begin by drawing on the key theories on the relationship between technologies and society. This approach illuminates and explicates academic conceptualisations of cyberspace. The next subsection of this chapter examines the key underlying social theories that are employed to understand and explicate cyberspace. The review thus far then allows for the ontological positions which underlie the study of cyberspace to be drawn out. Subsection four focuses on the examination and evaluation of academic conceptualisations of cyberspace.

On the surface it would be possible to begin by suggesting the presence of a classical dichotomy – that of believers and disbelievers; that there is a group of people who believe that cyberspace exists and another one that does not believe it does. Alternatively, one may suggest that there are those who believe that it does affect society and those who do not believe that it affects it. Then again,

one could claim that over time there was a move from a utopian to a dystopian understanding of cyberspace.

This all, however, would oversimplify the theoretical ontological and epistemological debates on cyberspace as it was not purely a move from modern to postmodern thinking. Rather, theorists' outlook from the start of inquiring cyberspace can be assigned to numerous ontological and epistemological positions. Instead of black and white, there are many shades of grey. Hence, before discussing specific explanations of cyberspace, I begin by outlining the conjectural positions underlying the theoretical and empirical conceptualisations of cyberspace.

3.3.1 Theoretical underpinnings

In the following two sub-sections I first outline techno-theory and what these tell us about cyberspace before considering the ways in which social theory is drawn on to explicate this new space of social interaction.

3.3.1.1 Techno-theory and cyberspace

For purpose of discussion one can group techno-theory approaches to cyberspace into the following perspectives: Utopian futurism, technological determinism, media determinism, social constructionism / constructivism, and political economy. These perspectives in this order reflect the range of theoretical underpinnings, from the cyber-enthusiasts to the cyber-critics. Furthermore, these positions have not been created through and for the study of cyberspace; instead they are

approaches that have been developed by theorists studying the relationship between society and technology and vice versa.

At this point it is worth mentioning that the review will demonstrate that cyberspace and the Internet as new technologies have been invested with the theoretical pre-dispositions outlined in the following sections of this chapter and thus take shape depending on the positions' ontological and epistemological outlook.

Those basing their ideas on utopian futurism define cyberspace as the decisive antidote to the dark side of society. It is to ultimately free us from poverty, suppression, inequality, and even wars. It does this by offering anonymity coupled with freedom of expression, and a global flow and access to information, therefore creating the ultimate democratic, informed, free, and powerful individual. Cyberspace is understood to be the final socio-political and cultural equalizer.

When applying technological determinist understanding to cyberspace we arrive at a technological space that is real and that

> "will lead to the formation of new communities, it will lead to changes in business practice, it will change how we live our everyday lives" (Kitchin and Dodge, 2001:25).

The emphasis is very clearly on society having to adapt to the technology, rather than on society appropriating cyberspace to shape it in a way that renders it useful and beneficial to society.

Media determinists argue that the Internet and cyberspace are thus technologies that if they do not directly change the social world, they still enable or facilitate change. They change the world by creating new forms of communication in a parallel, independent world that change the way the 'real' world is organised. The main criticism, which also applies to technological determinism in general, is that it ignores the social context within which technologies emerge. Media determinism cannot tell us how and why communication technology - here the Internet and cyberspace - develops, or why and how it is appropriated by social actors.

Cyberspace, viewed from the perspective of social constructionism/ constructivism, is a social space created by social actors continually developing and appropriating technological tools (i.e. Internet, computers, programs) in a reflexive process that occurs within a particular cultural and socio-political context.

> "Cyberspace, therefore, is a social artefact, as it mediates a series of social interactions and is itself a product of social mediation" (Kitchin, 1998:59).

While this approach does not deny modern communication technologies' impact on society it realises that the kind of impact and its extent heavily depend on how users make sense of cyberspace and how their lived context allows them to appropriate this technology. Cyberspace is deeply embedded in, instead of neutral and uninfluenced by, society.

A different insight is offered by communication determinism. According to this position the Internet is the technology that is appropriated by users and through the way social actors use and assign meaning to the resulting communications, cyberspace emerges. Cyberspace then is the product of social actors using communication technologies in particular ways. The obvious issue with this approach is that it does not take into account how social actors and their social interactions are then influenced by the resulting technologies, because the individual is seen to be an independent entity that has absolute control and choice.

From a political economy perspective cyberspace therefore, is not the free parallel world that is to do away with wars, illness, and inequality, which is user driven, but a plain tool for economic transactions created by powerful economic and political interests. However, it is also a sphere of political debate and as a side effect can lead to democratisation. Political economy's analysis focus is centred

> "on seeking to identify and explain the relationship between cyberspace and capital and to chart the social, political and economic manifestations of such a relationship" (Dodge and Kitchin, 2001:26).

3.3.1.2 Classical social theories and cyberspace

The above 'techno-social' theories are extended by more classical social theory. In the following section the key social theoretical approaches to cyberspace are outlined. I discuss these in slightly more detail than the above 'techno-social'

theories as to illicit how their original ideas were adapted and adopted to explain cyberspace.

The term post-structuralism refers to the work of highly influential writers such as Derrida, Foucault and Lacan. While those three authors worked on different areas they shared a common philosophical outlook that can be traced back to the work of Nietzsche and Heidegger. Their work is poststructuralist because it disagrees with structuralism in that it is critical of the idea of structures and offers notions on language that go beyond of what structuralism is capable of.

Structuralism became influential in the 1960s and 1970s and believes that social structures take precedence over social actions. It is the "view that society is prior to individuals" (Abercrombie, Hill and Turner, 2000:348). One key example is Levi-Strauss' structural anthropology and semiotic analysis of cultural phenomena. Another example is Althusser's structural Marxism. Overall structuralism is less interested in the detailed study of a particular cultural group, its focus is on discerning "potential universals and common structures of the mind" (Marshall, 1998: 646). A further interest of structuralism reflected in the work of Saussure and Chomsky are the structural features of language. Of particular interest were the synchronic relations "between linguistic elements rather than, as previously in linguistics, engaging in diachronic, historical or comparative study" (Jary and Jary, 2005: 616). For structuralists the individual, language, knowledge etc. are the outcome of underlying structures and the product of relationships between these structures; the idea of the subject that acts and chooses was done away with.

Post-structuralism rejects the claim that it is possible to find structures in society that underlie the human mind or social relationships and it re-interprets structuralist assumptions about language and society as signifying systems (Jary and Jary, 2005). Of particular importance is the claim that

> "Language is the place where actual and possible forms of social organization and their likely social and political consequences are defined and contested" (Weedon, 1994:325).

Instead of just reflecting reality – language creates it. And further, while structuralism sees the truth in texts for post-structuralism that truth and meaning arise out of the interaction between reader and text (Sarup, 1988). Therefore, meaning, truth and knowledge are thought to depend on the context, as outside of it, they may be quite different. Furthermore, identity, rather than being subject to conscious and subconscious thoughts, desires and emotions is highly influenced by discourses. Thus, our life experience shapes our identity, but our experiences are understood through discourses.

There are some criticisms that are made of this approach. For example Marxists and feminists would argue that it ignores materiality –wealth. A further criticism is that post-structuralism promotes relativism. The problem that arises is that post-structuralism cannot claim to be any better than any other approach, because by definition all approaches are just alternative discourses and there is no possible means by which one could test one's superiority over another.

Derrida (1981) declares that writing is the first communication technology. He argues that it provides a way by which one can overcome time in two ways. Firstly, writing replicates the immediacy of speech and secondly, it aids memory. This means that writing creates presence; it makes the subject appear without being there physically. Real time substitutes real space. Transferring these ideas to the phenomenon of cyberspace and new technologies means that

> "as communication becomes more immediate absence/ presence and writing/speech distinctions lose meaning" (Nunes, 1997:168).

This is one example where post-structuralist propositions are important as several theorists draw on them when justifying and explaining the existence of cyberspace, which in its early phase was constituted purely of text; and they offer a different way of understanding identity formation in and effects of cyberspace on identity. However, as will be made apparent later on, the weakness of this approach of understanding cyberspace is that philosophically speaking it can only offer part of or one possible conceptualisation of cyberspace, and does not allow for a precise and conclusive explanation of this technological phenomenon.

It is argued that post-structuralism paved the way for postmodern theories of society. Postmodernism is thought by many to be "related in some way to the emergence of a new social epoch of post-modernity" (Thompson, 1999:223). Postmodernism, it is argued, has replaced modernism in the second half of the 20th century. The existence of Postmodernity is highly contested; some preferring to call it late modern times instead (Giddens, 1990 and 1991). Equally, some are

already calling the end of Postmodernity announcing the next phase – hypermodernity (Charles, 2005). Thus, it is difficult to pinpoint when Postmodernity existed exactly. Lyotard announced in 1979 that people lived in postmodern times since the early 1960s. Many argue for its existence pointing to 4 groups of key features (social, cultural, political and economic) that are different from modern times. Firstly, the social structure is far more complex and fragmented than in previous times. The dominating factor is no longer class but it is now alongside gender, and ethnicity. Secondly, in the cultural sphere there is an aestheticization of everyday life, the fragmentation of identity and there are different ways of experiencing place and time. Thirdly, there is a desire for the reduction of the state, a drive for privatisation and competition. Fourthly, the economy is based on a post-Fordist economic system.

Recognising the immense changes in society over the 20th century social theorists began to be more reflective about their epistemological approaches to understanding and explaining social life of the 20th century (Castells, 1996; 1996; 1997). There is a tension between those who believe that postmodernity can be accounted for within the framework of existing theories and those who believe that previous approaches cannot fully account for social changes associated with postmodernity and thus call for a postmodern approach – postmodernism. An example of the former is David Harvey (1989), a Neo-Marxist, who while recognising the fast pace and dramatic social change in some areas of social life still argues that these are to be seen as an outcome of capitalism. Examples of the latter are Foucault and Baudrillard, who while not quite comfortable with the

label of postmodernism, still believe that there is a new epoch in which it is impossible to offer general theories about the social world.

Postmodernism as an approach has been in use since the 1980s. Proponents reject the possibility of a general theory and a recipe for improving society, which means that modernist social theories have to be abandoned. Drawing on post-structuralism, postmodernists argue that since language is subjective and knowledge is based on language, knowledge cannot be trusted. All this meant that there is no more basis from which to produce knowledge about the social.

Furthermore, Postmodernity is a time when the myths of liberation and truth have lost credibility. In addition, people are thought to be far less influenced by their social background and socialisation than in modern times resulting in them being free to choose their identity and life style. The old lines of fragmentation based on class have been replaced by fragmentation through consumption. This creates 'imagined communities' in which the membership is

> "a function of taste, choice and commitment so that the categories are therefore fluid in relation to one another indeterminate at the boundaries" (Marshall, 1998:513).

Additionally, authors such as Baudrillard and Lyotard describe how postmodernity replaced modernist symbolic orders with new symbolic orders, by shifting from a 'productive' to a 're-productive' social order. Signs have begun to make up the world, the distinction between representation and the real is diminished.

Baudrillard (1988) notes how while driving looking through the windscreen the driver interacts with images 'on' the windscreen, thus transforming motion into a visual experience.

Applying these ideas to technology and cyberspace in particular means that the computer screen is equated with the windscreen of the car (Nunes, 1997). The computer becomes the car, its screen the windscreen and the Internet the highways where the hyperreal vehicle travels through a simulated world that as technologies develop, the simulation - the hyperreal - begins to replace the real. This is an influential basis from which many conceptualisations of cyberspace originate. Combining post-structuralism with postmodernism authors argue that

> "cyberspace is providing new, less formalising and formal, disembodied spaces where identities can be constructed and contested; cyberspace is providing a new locale for communities, uprooted from the traditional boundaries of place; cyberspace is providing explicit spaces of artificial realities" (Kitchin, 1998:64).

Another perspective that is applied to the study of cyberspace and provides two opposing understandings is feminism. Feminism can be traced back to the French Revolution; however, most commentators associate the work of Mary Wollstonecraft in the 18th century as the true starting point of the discipline, which has since grown into an approach consisting of many perspectives. It can take the form of a holistic theory, a socio-political theory, a social movement, or an ideology. Overall, feminism can be distinguished into three phases –first wave,

second wave and third wave feminism. First wave feminism is the term describing the type of feminism that had its origins in the 18th century but came into its own in the early 19th century. It is a social movement that had as its aim the equality of the sexes by extending women's rights through equal voting rights and equal access to education. One key group at the heart of this social movement were the suffragettes.

The late 1960s and 1970s then saw the rise of a more radical feminism - termed second wave feminism. It was more radical because its aim was to transform society as a whole. It was led by academics such as de Beauvoir (1949), Millet (1969), Greer (1970) and Oakley (1974) who adopted Marxism, psychoanalysis and anarchism amongst other approaches to show that women are systematically disadvantaged. They had a significant impact on sociology as a whole because they showed how the discipline failed to recognise the role and the life experiences of women in society. One key study is Oakley's (1974) work 'The sociology of housework', where she broke away from functionalist ideas of Parsons of the family as a unit, to show the struggle for resources, equality and the conflict of interest that was at the heart of the family unit. She especially showed that housework was equal to paid work and that women's suppression was structural. This type of feminist theory conceptualises technology and cyberspace as artefacts created by men, where men hold the means of production and design etc. using it as yet another technological means to subordinate women and even violate them.

Before discussing third wave feminism in more detail one has to make the reader aware of the fact that this term describes two different feminisms; one being academic and the other being a new social movement. The social movement of third wave feminism are the activities of women in cyberspace that are intended to use cyberspace to articulate ideas about femininity to carve out what some call 'grrrl identities'. This means that women are creating alternative discourses on what it means to be a woman in the 21st century, online. Beyond this these women reject previous academic feminism as they do not feel that their experiences and beliefs are represented by these accounts (Harcourt, 2004; Armstrong, 2004).

Academic third wave feminism, similar to third wave feminist movement, rejects second wave feminism because it ignored non-white middle class perspectives. This accusation is made especially in black feminism. Furthermore, in the 1980s and 1990s some began to combine feminism with post-structuralism and post modernism. Those combining feminism with post-structuralism where interested in how the female body is represented and suppressed in male dominated writing (Abercrombie, Hill and Turner, 2000). Combining it with postmodernism appeared to be rather difficult because postmodernists regarded feminism to be a product of modern social sciences. However, Hekman (1990) argues that there is enough similarity between the two to allow for postmodern feminism.

Postmodern feminism is similar to black feminism and the third wave feminist movement in that it denies the possibility of a singular theory that can explain the

position and experiences of women in society. Joining post-structuralism, postmodernism, and feminism creates a perspective that understands progress as the outcome of male dominated rationality and that wants to deconstruct male language and view of the world to allow for many discourses on femininity that are produced by women. This type of feminism, third wave academic and movement, perceives cyberspace as the space that allows women to deconstruct male dominated discourses on femininity empowering women to offer up alternative accounts.

Thus, when considering feminist conceptualisations two types of cyberspace are imagined, a male space in which and through which women are further suppressed and a potentially female space where women can free themselves from male domination. This is important to note and understand because cyberspace is created out of the imaginaries which accompany or precede it.

One further theory that is much relied upon in the study of cyberspace is that of social interactionism. Even though sociologist had already studied social interaction the structures underlying this interaction were not fully appreciated and studied until Ervin Goffman. Goffman was heavily influenced by three perspectives: symbolic interactionism, neo-Durkheimians, and social anthropology. The first two influenced his thinking in that they made him aware of the role of symbols and rituals in everyday life; social anthropology provided the research method (participant observation) by which he could study these (Marshall, 1998).

Goffman's interest was micro-sociology and his seminal text was "The Presentation of Self in Everyday Life" (1959), in which he developed a sociology of everyday life, seeking to understand and to explain, what are often considered trivial, encounters between social actors. Giddens (1993) offers two reasons for why the study of even trivial day-to-day interaction is important. Firstly, the majority of our daily social activities are repetitive and are made up by social interactions such as face-to-face interaction. This gives structure and form to what we do. Secondly, studying these helps comprehend social systems and institutions.

Goffman (1959, 1963, 1971) inter alia argues that social interaction is governed by an interaction order, a kind of public order that is based on moral norms. This interaction order allows for interaction to occur in an orderly way, thus creating social order –albeit it order that is always at risk due to possible misunderstandings, shame and disagreement. Drawing on his concept of acting he then argued that social interaction performs a ritual - interaction ritual - that contains ritual codes that allows social actors to enact a shared social reality.

To explain this he used the analogy of stage acting and thereby created the dramaturgical perspective for sociology (Marshall, 1998). This perspective suggests

> "studying social interaction as if those involved were actors on a stage, having a set and props. As in theatre, in the various contexts of social life there tend to be clear distinctions between front regions (the stage itself)

> and back regions, where the actors prepare themselves for the performance and relax afterwards" (Giddens, 1993:113).

When thinking of technology through the lenses of social interactionism its rootedness in symbolic interactionism comes to the fore. Technology is something that is used as a prop in social interaction. People use it to negotiate and facilitate social interaction. While it cannot tell us about the practical use of technology, it strengthens the arguments that social constructionism and constructivism make. What about the Internet and cyberspace? With regards to the Internet and cyberspace social interactionism tells us about how people use the technology to communicate with each other and it sheds light on how people's interaction creates spaces for social interaction and how social actors act within these spaces.

One of the strengths of Goffman's approach is that it allows us to understand and explain face-to-face interaction. The application of his ideas to the Internet and cyberspace therefore appears misguided as in the beginning there was no face-face interaction, and the dominant form of communication in cyberspace is still faceless. Even if we see a video image of a face, is that equal to the type of interaction that Goffman based his ideas on? Still, applying social interactionism to cyberspace is very useful because people are still applying ways of managing the presentation of their self in this technologically facilitated space. These ways may differ from those observed by Goffman, however, his theory allows us to identify, understand and to explain them.

The cyberspace that emerges is a space that is situated in space and time, where people interact with each other, where the front region -stage- is the text/ image on the screen and the back region is the place where the individual is sitting in front of the computer screen. It is a space where people have to work less hard on civil inattention, that lacks non-verbal communication and the face has lost importance. It is because of these factors that break with Goffman's original ideas on social interaction that cyberspace is sometimes regarded as a new space for new social interaction where new selves emerge.

3.3.2 Is cyberspace a different and new research environment?

Having identified the underlying theoretical positions, I now proceed to study how these have been applied by social scientists to make sense of their new research environment -cyberspace. Markham points out that the question of 'where is the field?' is very important. It affects:

> "(1) what we consider important in the collection of information about the Other; (2) how we interpret their actions and discourse; and (3) how we represent them in the research reports" (Markham, 2004:144).

The definition of the field poses big problems to online social researchers. When reviewing the literature one cannot help but be left with a sense of confusion on whether this field is virtual or real, embodied or disembodied, offline or online, parallel to, or an extension of the physical world. What makes a definition of cyberspace so difficult is that it is a social environment created by its users, Internet Service Providers (ISPs), regulators, organisations, governments,

legislation, cultural, media and academic conceptualisations. This creates a rich range of narratives that only share one key tenant: that cyberspace exists or not. What it means, how it works, what it can, should or ought to do is highly disputed.

3.3.3 First steps in conceptualising a new research location

When reviewing the academic definitions of cyberspace from 1992 until today there are several points that can be made. First, there have been tensions between those who are cyber enthusiasts, those who are cyber sceptics and then those who are somewhere in between. Second, consequently there is not one single cyberspace that emerges but a multitude of different cyberspaces that, a lot of the time, cannot be quite reconciled with each other. Third, while there are some who argue that it does not exist the majority agrees that there is a cyberspace. Fourth, there is disagreement on where this space actually is. Fifth, there is some confusion arising out of using the Internet and cyberspace as synonyms for each other. Sixth, there is disagreement on what type of space cyberspace is. Seventh and partly resulting of the point before, there is disagreement on the social interactions that can occur in cyberspace. Eighth, there is disagreement whether the online social interaction has positive or negative outcomes.

One of the first, certainly the most quoted, definition of cyberspace is offered by Benedikt who writes:

> "Cyberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multi-dimensional, artificial, or 'virtual'

> reality. In this reality, to which every computer is a window, seen or heard objects are neither physical nor, necessarily representations of physical objects but are, rather, in form, character and action, made up of data, of pure information. This information derives in part from the immense traffic of information that constitute human enterprise in science, art, business and culture" (Benedikt, 1992:123).

One year before that Stone (1991) defined cyberspace as a virtual reality with goggles. In 1995 McDonough brought the academic attempts to understand and define cyberspace to the point.

> "…there is an immense degree of confusion and disagreement about the exact meaning of the term 'cyberspace'" (McDonough, 1995).

There are however, doubts on whether this sphere of interaction actually exists in the first place. Asking the question of 'does cyberspace exist?' recalls two previous dilemmas. First, an example from Christianity of having to touch something for it to be real – thus the question of physicality. Second, the age old debate in sociology of is there such a thing as society and where is it? This is slightly abbreviated into 'does cyberspace exist and where is it?'. In order to gain a better insight into the question of its existence some have looked at the ways in which it may be created. In answer to this question some argue that cyberspace is a linguistic construction. They base their argument on Derrida's (1981) ideas as outlined above.

The central tenets are that users use spatial metaphors to locate their social interactions via the Internet and drawing on post-structuralism that presence can emerge out of text. One example of this argument is McDonough definition of cyberspace:

> "Any form of synchronous, interactive digital communication which deliberately employs and relies on a metaphor of shared spatial location in order to orient participants within the communication domain to each other and /or other entities/ 'objects' within the domain" (McDonough, 1995).

McDonough (1995) then offers us two possible reasons for why certain groups interacting via the Internet may have to use spatial metaphors and thus creating cyberspace. He tells us that one group who does need a cyberspace is that group of Internet users whose communication and interaction places a lot of emphasis on the space itself in which their communication and interaction occurs in. Another group that needs a cyberspace and creates it through spatial metaphors are those users who while not focusing on spatiality itself still feel the need to locate their interactions in a particular space for their interactions to be plausible and meaningful.

Grounded in a technological determinist view Chesher tells his audience that users do not create cyberspace but that "computers create digital domains: parallel universes where events occur outside the usual physical spatial constraints" (Chesher, 1997:79). He indicates that he is aware of why his colleagues argue that cyberspace is spatial, however, denies the possibility of real space to emerge

out of spatial metaphors that are used in rhetoric on computers and the Internet. Chesher offers a very interesting reason for why there cannot be any space in cyberspace. He argues that due to the speed of real time communication afforded by computer-mediated-communication space is reduced to time.

> "Space in the physical world becomes time in the ontology of the digital domain. Distance is manifested in invocational delays of nano- or microseconds" (Chesher, 1997:85).

If social actors can communicate with each other at such speed their physical geographical location becomes irrelevant. Therefore, Internet communication does not create cyberspace but instead destroys space creating presence. This is reminiscent of Castells' (1996) ideas on the space of flows. Simply put, everything that is in cyberspace is here, without distance.

When reviewing his argument's theoretical basis several interesting points can be made. At first it appears that he rejects post-structuralism because he argues that text and speech cannot create a real space – cyberspace. However, he then returns to post-structuralism by following Derrida's (1981) point that language creates presence. Therefore, instant communication reduces space to time, and ultimately creates presence, but not somewhere half way in a cyberspace but at the respective geographical location of the users. Does this mean that people exist in two places at the same time? So instead of cyberspace as an in between meeting place modern communication technologies create clones of ourselves? His argument is compelling, however, some questions must be asked. If he is

right, where are the chat rooms and discussion forums, where are the online pc gaming worlds?

While Chesher's (1997) argument represents an interesting philosophical and sociological undertaking, it is not taken up by the majority of his peers. Based on the socio-spatial ways in which they conceptualise cyberspace I suggest that this may in large part be true due to the fact that they see narratives grounded in cyberpunk as the most useful tool in approaching and understanding cyberspace.

Thus the dominant notion in discourse on cyberspace is that cyberspace lies somewhere beyond our computer screens. There are different ways in which the computer and the screen are thought to provide access to cyberspace. One of the first and resonating ways to describe it is offered by Turkle (1996) who talks about users stepping through the screen into cyberspace. The screen is like a window or door that the user through a process of disembodiment can step through into cyberspace. Another way of describing it is offered by Virilio (1989) who, drawing on Baudrillard's and Barthes' ideas, calls the computer the 'last vehicle'. The computer as a whole has been turned into a hyperreal vehicle that permits travel through a simulated hyperreal world.

This notion of two worlds is reinforced when authors such as Walther and Boyd (2002) use the terminology of online and offline interaction. The observer has to – at least at face value- assume that there are two distinct spheres of social interaction; that there is the space of the real world and then the space of

cyberspace. This means that the separateness is quite clear cut. However, Kendall writes "Individuals exist and participate in offline social contexts both sequentially and simultaneously with their online participation" (Kendall, 1999:60). Consequently, the separateness from the real world is reduced and cyberspace appears as a further extension albeit a new one of the existing social world. More succinctly, cyberspace is just another sphere of social interaction, in which social interaction occurs based on the means of communication that are available. Maybe, one can draw on Lee's (2005) ideas on separability to explain this. While he is applying this to explicate the relationship between child and parent, the core of his idea is that there is a relationship between two entities that allows both to exist and function to their own rules to a large extend while still being linked.

In an attempt to resolve the uncertainty some distinguish the real and the virtual by drawing on a further dichotomy of wires and the mind. The Internet (the wires, computers and networks) represents the real while cyberspace is thought to reside in the mind. One commentator argues that "cyberspace lacks a physical location beyond our computer monitors and keyboards …" (Borer, 2006). Thus the location of cyberspace is in our minds. This has drawn some commentators to the view that cyberspace is a hallucination. It is a world that is dreamt up and shared by its users. However, Borer (2006) argues that "defining cyberspace as a 'consensual hallucination' is inadequate for describing the real life domain we commonly refer to as cyberspace" (Borer, 2006). Therefore, while the notion of cyberspace as existing in our minds is not rejected, to think of it as a hallucination is.

Many theorists have drawn on the virtual vs. real dichotomy as another means by which to distinguish and explicate the distinction between the real world and the virtual world. This way of tackling the issue is grounded in cyberpunk fiction. The terminology and the ways in which cyberspace is defined as a virtual parallel world all stem from fictional conceptualisations of this social phenomenon.

3.4 Mixing cyberpunk and social theory

It was from there that the idea of cyberspace spread via the media, film, public and political debate, all of which have drawn on Gibson's initial ideas to understand and then conceptualise cyberspace. Looking at the academic definitions in this chapter thus far one can clearly see how very influential these cultural understandings for academic debates are. Still, while initially useful in explicating technologically mediated social interaction it has arguably led to many misunderstandings and uncertainty about cyberspace. This is because the range of possible narratives about cyberspace that can be subscribed to in the absence of physical/ hard evidence to the contrary.

Borer is highly critical of what he sees as the postmodern exaggeration of the "sociality of cyberspace and the interactivity between the 'virtual' and the 'real'" (Borer, 2006). His attack is mainly aimed at Turkle (1996) who he singles out as one of the main 'culprits'. However, there are several problems with his argument. First, while he is right to argue that early postmodern accounts where too utopian, he fails to recognise the clear shift in postmodern accounts. Second,

he does not remember that Turkle herself tried to break down the distinction between the 'real' and 'virtual'.

He appears as the defender of the 'real' as he attempts to fend of postmodernist claims that due to disembodiment face-to-face interaction has been made obsolete and that we have submerged ourselves into the virtual; something he insists on being inauthentic and simulated. Borer sums up his argument by arguing that postmodernists

> "…fall into the trap of reification, envisioning cyberspace as an object unto itself, a self-relational and self-supported realm of dehumanized hyperreality" (Borer, 2006).

Borer does two things, he questions the idea of the power of the virtual and he rejects the objectivist idea that cyberspace is an entity that can exist outside of social interaction. His work is one example of social constructionism applied to technology.

At the heart of the distinction between 'real' versus 'virtual' is the belief that the virtual is not real because it has no physical manifestation and therefore social interaction in cyberspace is artificial or ephemeral (Fernback, 1999; Talbott 1995). However, there are others who disagree with the above statement. Nunes (1997) offers a very different assessment of the virtual by applying Baudrillard.

> "Cyberspace abandons the 'real' for the hyperreal by presenting an increasingly real simulation of a comprehensive and comprehensible world" (Nunes, 1997:163).

Thus the model of the world becomes the world itself. In essence then the virtual known as cyberspace has moved beyond being an alternative sphere or parallel world to become as good as and even realer than the real. By 1997 Hillis writes that virtual worlds are

> "being positioned as the ideal public sphere for imaginative subjectivities believing themselves virtually freed of bodily constraints" (Hillis, 1997:20).

This latter argument leads us to another way of understanding cyberspace by describing the nature of social interactions within it. Thus instead of focusing on the space or non-space as such, one can find out about the space by learning about the nature of the interactions within it. For example, if interactions within it are free of gender biases that would suggest that cyberspace is distinct from the 'real' world and represents a more equal social sphere. Overall, cyberspace seen from the different positions emerges as a space of two extremes. Either it is thought of as a space that inhibits social interaction or a space that encourages social interaction; or it is a space of gender bias or freedom from gender bias; it can be a space of freedom of speech engendering democratisation or a space representing the ultimate means of surveillance. To illustrate this point I draw on the examples of anonymity and gender.

One aspect of social interaction that has been dominant in early discourse on cyberspace that is still influential today is that of anonymity. Cyberspace is thought of as a space that allows anonymous social interaction. Sassenberg and Kreutz (2002) discuss two theories in relation to anonymity in cyberspace – the

RSC model and the SIDE model. The RSC or 'reduced social cues' model is solely used by critics of cyberspace. It argues that because during interaction in cyberspace less information is communicated than in face-to-face interaction computer mediated communication is less of a social interaction. This means that cyberspace is a second class anonymous sphere that is second to the real world in which untrustworthy accounts of identity are created. The second model they discuss that is of relevance here is that of 'social identity deindividuation' (SIDE). The SIDE model is based on two variables of social influence; a cognitive aspect and strategic aspect. At the heart of the SIDE model is the idea that with increasing anonymity, less information about communication partners is available which "…results in stronger attachment to rules of behaviour (identification) associated with personal or social identity" (Sassenberg and Kreutz, 2002:216). The result is that people while in cyberspace exhibit greater adherence to social norms than in face-to-face interaction. This means that instead of being more honest people appear to tend to give socially desirable responses (SDR) in cyberspace at least until they have gathered more information about their interaction partner (Bosnjak, 1997).

Interestingly, Rietz and Wahl's (1999) findings suggest something different. They found that people were less likely to give SDRs in web based surveys than in pen and paper ones. This does not mean that Bosnjak (1997) is wrong; rather it suggests that depending on the type of communication and the perceived identifiability affect the level of SDR. Therefore, one has to be specific about the context and cannot necessarily reduce it to the face-to-face versus computer

mediated communication dichotomy. Kendall (1999) is another researcher who rejects the idea that cyberspace is an anonymous space. He associates anonymity with contextlessness, and because "online forums do not provide contextless spaces free from expectations about identity or from challenges to identity claims" (Kendall, 1999:66), cyberspace is not truly anonymous. Nonetheless, using these ideas cyberspace emerges as an anonymous space that can be 'better behaved' than the real world and instead of freeing us from social constraints actually make us even more bound by them.

It is partly out of the position one takes on whether cyberspace offers anonymity or not and whether it has bad or positive effects that understandings of other aspects of cyberspace are formed. One example of this is the issue of gender. Sociologists have established that gender inequalities exist in the offline world. In the online world, however, many theorists argue, these inequalities fall away. One of the key reasons is that women can control the information about their gender and thus participate in social interaction freely. Whether hiding one's gender is the same as equality is often overlooked. Furthermore, cyberspace provides a space for third wave feminism and the often called phenomena of the 'mouse-wife' is argued to do away with experiences of social exclusion and loneliness experienced by housewives described by Wilmot and Young (1962), Oakley (1974) and Goldthorpe et al. (1969). Nonetheless, Poster tells us that while gender cues are absent in cyberspace this "… does not eliminate sexism or even the hierarchies of gender that pervade society in general" (Poster,

1997:222). Here again we are faced with a dichotomy of underlying understandings and attitudes towards cyberspace.

This section shows that academics have made many novel attempts at understanding and explicating cyberspace by drawing on the whole range of social theory and even cyberpunk fiction at their disposal. In their pursuit they take many different ontological and epistemological starting positions. This leads to the emergence of many different kinds of ways to understand cyberspace. Not all of these notions are fully reconcilable. The position that I propose to discount outright is one that argues that cyberspace does not exist. There is too much evidence that social actors have created a social reality in which cyberspace clearly does exist to allow anyone to pretend that it does not. Returning to my earlier point that not all notions are entirely reconcilable they still share the belief that cyberspace does exist. They may disagree on how it has come about, what its actual forms are, how we enter it, how we interact in and via it, whether it frees us or further enslaves us, and whether it has an overall positive or negative effect on real life. There is, nonetheless, a core to their understanding of cyberspace that is shared. The difference between accounts appears to rest on whether one is an optimist, pessimist or somewhere in between. When reviewing the above section I am able to offer a general academic conceptualisation of cyberspace.

Cyberspace is:

- Constantly changing and evolving.
- A parallel world that is deeply embedded in society.

- A social artefact.
- Potentially the anti-dote to the dark side of society.
- Potentially replicating and magnifying the dark side of society.
- A space that offers potentially new forms of identity and community.
- Lawless and devoid of regulation and thus democratising yet posing dangers.

This general understanding of cyberspace covers very similar grounds to the fictional and public conceptualisations discussed before and thus poses similar outcomes for current online social research guidance as already discussed above. What makes the academic definition of cyberspace so important and problematic for current guidance is that this is what our guidance is by and large based on. This is problematic because different positions on cyberspace will bring about different understandings of morality of and risk in cyberspace and thus determine in how far current social research ethics guidance can manage this risk. For example, if we constructed cyberspace as a consensual hallucination we would arrive at a different assessment of risk and need of guidance than when constructing cyberspace as an information network. To counter this, one would have to base online social research guidance on the general academic conceptualisation outlined above. Doing this would permit to compose guidance that takes into account the research environment's fundamental realities while leaving it flexible enough to address whether it is a positive or negative context. The question still remains in how far current social research ethic guidance

accommodates these general academic conceptualisations and thus its ability to manage risk in online social research.

One of the key things to emerge from this section is that while politicians' and cultural/popular conceptualisation engage with its legal, regulatory and coding reality, social theorists do not consider the legal and regulatory realities when defining cyberspace. I realised this because this was one of the key matters that I interrogated the literature for. It is true that there is much written about how the lack of legislation and regulation leads to freedom of speech and a new era of democracy (Lax, 2004). However, these accounts are based on utopian conceptualisations of cyberspace that can be traced back all the way to cyberpunk fiction. There is no discernible attempt by the wider field to question these assumptions. Only a few have addressed key issues of legislation regarding the age of consent; the right to privacy; communication interception; public vs. private space; legal jurisdiction; and data protection.

3.5 Mind the gap

The realisation of the applicability of the Internet and cyberspace as a research tool for social research has brought about a sharp increase in social research being carried out via or in cyberspace. These activities have caused some debate within mainstream social research in general and within online social research in particular about its merit, and brought about disagreement and uncertainty about the applicability of 'tried and tested' traditional methodology, and ethics in this

'new' research environment. There is no clearly defined framework for harmonizing the different positions.

The key findings of this chapter are:

- Powerful social actors heavily rely on cyberpunk and fictional conceptualisations to make sense of cyberspace and computer-mediated communication.
- The cyberspace that emerges out of these discourses is an extension of the offline world into an online world where the realities of the offline are amplified to the extreme
- Academic conceptualisations of cyberspace are also (surprisingly explicitly) based on fictional and popular, and while disagreeing on its expressions still agree that it exists.
- Cyberspace is a 'new' and 'different' environment. However, to what extent is contested.
- In such an amplified social space it is at this point difficult to predict in how far current social research ethics guidance can manage risk in online social research.
- Academic conceptualisations of social researchers are not considering the legal and regulatory framework of cyberspace sufficiently.

Overall social theoretical conceptualisations mean that it is improbable that cyberspace is the sphere of a radically new and different morality that creates new and different risks that current ethical guidance cannot manage at all. There is a matter of amplification that potentially poses known risks in new or amplified ways

that may well stretch current ethical guidance's ability to manage them. The real gap, however, lies in the lack of engagement with the legal and regulatory reality of cyberspace. So far social researchers appear to have entered this 'new' and 'different' online research environment by innovatively drawing on techno-social and social theories, all the while being heavily charmed by cyberpunk narratives.

However, while doing this they have neglected to realise and thus recognise the legal and regulatory foundation of cyberspace, which results in at best incomplete theoretical conceptualisations of the online research environment and thus has a potentially serious knock on effect on whether current ethical guidance can manage risk effectively or not.

Thus, I argue that we have to add a legal and regulatory element to our social theory understanding of cyberspace and then reassess the types of risk that may emerge in online environments and research, and in how far current ethical frameworks of social research can manage these risks.

Chapter 4:

The legal conceptualisation of cyberspace

4.0 Introduction

One of the key points that the previous chapter established is that current academic literature on online social research in general and its conceptualisations of cyberspace in particular do not engage with the legal and regulatory conceptualisation of cyberspace. However, the factors that brought about the thematic shift of my thesis suggest that the ways in which laws and regulations shape the Internet and cyberspace are not to be disregarded. Thus this chapter's objectives are to investigate how legislation and regulations conceptualise the Internet and cyberspace; to establish how far they actually do shape and impact upon the Internet and cyberspace; and to begin considering what this may mean for the ethical guidance's ability to manage risk in online social research.

To carry out this investigation I scrutinised the literature on the regulation and legislation of the Internet and cyberspace, and examined the ways in which legislation and regulation themselves either directly define the Internet and cyberspace or what kind of 'new' and 'different' sphere of social interaction their structuring of mediated social interaction creates.

4.1 Brief history of legislating cyberspace

As outlined in chapter three the ways in which many theorists and researchers construct cyberspace may suggest that it is free from legislation and regulation.

However, this argument is deeply flawed. In fact cyberspace was regulated and legislated for before it even became a reality. First of all the Internet, thus the technology that enables cyberspace in the first place, was and to some extent still is the brain child of the American government. The Internet was the outcome of political policy and very much subject to US legislation. The US government created the institutions that built the Internet and it also decided when other national networks were allowed to join it (Dodge and Kitchin, 2001). There is, however, one further way in which cyberspace is created and controlled that lies beyond legislation and regulation – code. Lessig (1999) identifies code as further evidence that cyberspace is not lawless. He argues that one way in which cyberspace is legislated for is through the coding of the Internet and other communication technologies. It is code that creates the environment in which social actors can interact and therefore if the government controls the code then cyberspace is not lawless but can be and is controlled by the state.

Interestingly, up to the point when the national networks were joined to each other in 1988 there was a clear understanding that the networks were under the jurisdiction of the respective governments which had absolute control over these networks. Also, these networks were not considered as creating a separate social sphere. Instead they were thought of as large databases that were accessible from computers connected to the network not all that different to accessing one's own hard drive. However, we still do not consider ourselves as going somewhere when searching for a document on our own PC.

There was a marked shift in perception after the networks were joined. With the increase in private business influence on the networks, Western legal understanding of networks changed too. From the 1980s onwards legal understanding of cyberspace became problematic. The governments were no longer the sole owners of the computer networks, and the appearance of cyberspace put into question legal boarders and thus legal jurisdiction. At this point it would have been possible to still consider the global Internet as national networks that were connected at several points with the legal jurisdiction falling into the country of where the offending PC was situated. Johnson and Post point out "Traditional legal doctrine treats the Net as a mere transmission medium that facilitates the exchange of messages sent from one legally significant geographic location to another, each of which has its own applicable laws" (Johnson and Post, 1996:1368). One example of this approach is the UK Computer Misuse Act (1990).

However, two problems developed. Firstly, social actors through their interaction via this new technology drew on much older metaphors stemming from the time of the telegraph to describe their experiences online (Standage, 1999). They called this sense of space – cyberspace. Therefore, territorial law was put into question. What is this cyberspace? Where is it? and who owns it? were all questions of ever increasing importance. One answer to this issue would have been to conceive cyberspace as

> "a distinct 'place' for purposes of legal analysis by recognising a legally significant border between cyberspace and the 'real world'" (Johnson and Post, 1996).

The border into cyberspace is the screen and passwords. However, this approach still does not solve the issue of jurisdiction. What it does is to offer one facet of the legal conceptualisation of cyberspace – cyberspace as a separate world that is in need of its own laws. Secondly, returning to Lessig's argument on code, now that governments are privatising the Internet and thus "if [the code] is not owned, control is much more difficult" (Lessig, 1999:7). Even then, cyberspace is not lawless.

> "When commercial interests determine the architecture, they create a kind of privatised law" (Lessig, 1999:59).

Over the next decade and a half governments, courts and the legal profession in general tried to answer the question of what is cyberspace by uncovering its nature. What is most striking, however, is that while trying to unearth cyberspace, they actually played an enormous role in creating cyberspace (Johnson and Post, 1996; Lessig, 1999). Putting it simply, they did this by applying the formula 'if cyberspace is this, then you must act in this way'. Doing this the legal conceptualisation of cyberspace became the dominant even though not uncontested force in defining cyberspace. It did so mainly through defining acceptable parameters of social action during social interaction in cyberspace. Examples are: defining cyberspace as consisting of many places; setting rules of

economic activity and trying to engender trust; protecting individual's privacy and right to freedom of speech while defining cybercrime and cyber-terrorism.

The other way in which cyberspace was regulated for was through 'private laws' (Johnson and Post, 1996). Many governments due to their uncertainty of jurisdiction in cyberspace decided to 'force' private companies that are involved in cyberspace to self-regulate. Several laws have been passed and are continuously updated to keep up with technological and political developments that indirectly legislate and regulate cyberspace. Examples of these laws are: Teledienstgesetz 1997 (GER); Telekommunikationsgesetz 2004 (GER); Digital Age Communications Act 2005 (UK); Jurisdictional Certainty of Digital Commerce Act 2003 (US); and the Telecommunications Act 1996 (US). Private laws/ regulations take on the form of 'terms of service' of use that users have to agree and adhere to and the codes used to create the actual online environments. All of these actions meant that whatever real fluidity and flexibility cyberspace may have potentially possessed had become moulded into a legislated and regulated settled form. Settled not in a sense of unchanging but changing in a controlled fashion. The laws, whether public or private, define the architecture of cyberspace.

After the initial hesitation had passed, governments began to construct a legal understanding of cyberspace. What stands out is the fact that Western governments apart from America and Germany chose the indirect way of legally understanding cyberspace. They did so by amending old legislation to make them applicable to similar offences carried out via the Internet or in cyberspace. Good

examples of this are provided by UK legislation such as the Computer Misuse Act 1990 and the Intelligence Services Act 1994. So far no UK Act has been passed that contains the term cyberspace either in the title or in the actual legal text. The American and German government, however, while amending older legislation, also created a whole host of Acts that were specifically about cyberspace. Examples are the Enhancement of Privacy and Public Safety in Cyberspace Act (1984/6/94/96); Child Online Protection Act (1998); Cyberspace Electronic Security Act (1999); Global Internet Freedom Act (2003); Online Privacy Protection Act (2003); Online Freedom of Speech Act (2005).

Although the aforementioned Acts have not been passed yet or have been blocked by the Supreme Court, they nonetheless represent one way of legal conceptualisation of cyberspace and the fact that they were contested further warrants their inclusion. What is more important here is to recognise that in American law, cyberspace appears to be considered a separate world that is in need of its own legislation. In the other Western countries cyberspace appears to be considered an extension of social spheres of interaction that are basically covered by previous laws yet offer new ways of committing the same crime or for expressing the same social issues. Furthermore, governments appear to prefer a laissez-faire approach encouraging the market to self-regulate. Thus they do not feel the need to create new cyberspace legislation rather they extend existing legislation and step in if the market fails to self-regulate.

Therefore, legal conceptualisations at this stage of my analysis appear to be contested. What they have in common is the recognition of the existence of cyberspace and global Internet networks. They also agree that cyberspace poses important questions with regards to legal jurisdiction, definition of crime, human rights, privacy, and freedom of speech. The cyberspace that emerges is a space that consists of places of social interaction that are subject to some, yet not enough, legislation; and that are subject to at times conflicting legislation. Each place may have its own rules and norms, and it can be a source of danger and crime by granting anonymity to criminals. This means that cyberspace can have a negative impact on the security and well-being of the real world and society.

4.2 Where is legislated and who legislates?

Having offered an overview on the development of the legal conceptualisation of cyberspace I will now address the question of where this legal conceptualisation is conceived and by whom. This is important as it gives deeper insight into and understanding of what cyberspace is and how it needs to be defined. When compiling a list of laws on cyberspace it is apparent, that there are several levels at which cyberspace is legislated for. These are: the international level (UN, G8 and EU); the multi-national level; the national level and the regional level (States, Bundeslaender).

Let me offer an illustration of this. The council of Europe has put forward a convention on cybercrime in 2001. This was then signed by 34 member states and 4 non-member states (US, Canada, Japan and South Africa) and stands as an

example of the international level. The convention itself called for the creation of multi-national consent on the definition of cybercrimes and a change of domestic laws to allow for greater international cooperation. This led to multi-national agreements. On a national level it meant that governments implemented the convention into domestic laws; examples are the Telecommunications Acts of Germany (1996/7/8), Spain (2002), Australia (1997), and New Zealand (2002). At the regional level we can draw on the example of the Californian Online Privacy Protection Act (2004).

What appears to occur is that different levels have different purposes in the development of cyber law. International bodies (UN, G8, EU) tend to address cyberspace in a more general way. At this level political leaders gather, sometimes with representatives of businesses and interest groups to discuss 'the bigger picture'. Examples for this are the UN Information Technology conferences in Geneva and Tunisia, the 2001 G8 meeting or the EU conferences on the convention on cybercrime. They also tend to commission reports such as the 1998 COMCRIME study funded by the EU. Based on their initial actions and remit that they have set themselves we can deduce that cyberspace to them is a global phenomenon criss-crossing borders and jurisdictions, that is better left to self-regulation. This position has moved on somewhat especially the EU is more pro-active now. Examples are the Convention on Cybercrime (2002) and its guidance on the protection of intellectual property in (2004). These conventions have to be implemented by the member states into national laws. However, national laws or approaches to cyberspace also influence international bodies. A recent instance is

that of the international debate on the official regulation of Internet domain names, where the US government has basically over-ruled international desire to move control away from the ICANN to an international independent body.

Mostly, however, the International conventions and legal conceptualisations of cyberspace are applied to domestic law. On a national level the legal conceptualisation of cyberspace is also influenced by a particular country's economic and political self-interests and needs. As outlined above governments have had to decide whether they wanted to be more pro-active or 'laissez-faire' in their approach. In most instances they have opted for a mixed approach. They have up-dated key legislation and put new legislation into place where there were gaps to either deal directly with a particular concern or to encourage self-regulation. Issues that are the driving force behind legislating cyberspace are crime, trust and security. I offer a few examples as means of illustrations.

Relatively early on governments and businesses realised that in order for the economy to use the Internet and to make profits, cyberspace had to be a safe environment. A lot of the debates were about whether the government should be the regulator or whether the government should regulate the cyberspace companies into self-regulation. As example I remind the reader of the aforementioned letter written by the Metropolitan Police to over 140 UK Internet Service Providers (ISPs) in 1996 and statements by Germany's former Home Secretary Schily (above at s.3.2.2.2)

> "This list [of pornographic news groups] is only the starting point, and we hope with cooperation and assistance of the industry...to be moving quickly towards the eradication of this type of newsgroup from the Internet. We trust that with your cooperation and self-regulation, it will not be necessary for us to move to an enforcement policy." (Metropolitan Police Service, 1996, cited in Anderson, 1998:23)

Again cyberspace is imagined as a separate lawless social sphere that offers great benefits as long as it is properly regulated. In the UK the government adopted and still does take a laissez faire attitude and only intervenes into cyberspace regulation when absolutely necessary. There are, however, other countries such as the US or Germany who take a more active role. An example of this is the statement by the former German Home Secretary Schily during a G8 meeting on 'Security and Trust in Cyberspace' (2000) demanding a strong international regulation of cyberspace. Expressing what many of his colleagues felt - that cybercrime had become a threat to public security and the information society. The conference ended with a strong sense that cyberspace must not remain a lawless space. The way forward was international legal consent and clearly defined laws.

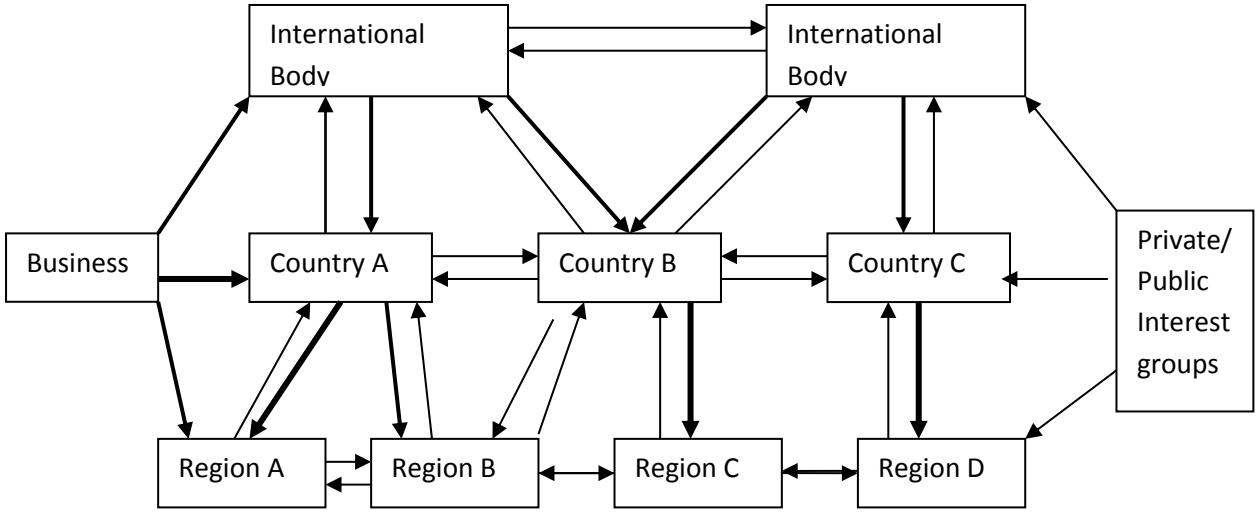
Even though we are by far more familiar with the activities of certain suppressive regimes, Western governments also actively impact on the social interactions that are possible online (Karatzogianni, 2010). One example are the different interactive opportunities available to Yahoo! Users in France, Germany, the UK

and the US. US users may access chatrooms from within its messenger service while UK users cannot. In France entire sections of Yahoo! are inaccessible because they contain 'controlled materials' due to government regulation and a decision of the County Court of Paris (Fowler, Franklin and Hyde, 2001).

Legislation is created at two levels the national and the regional. Examples for this are those acts produced by US states or German Bundeslaender. There is a complex interplay between national and regional/local legislation that makes the question of jurisdiction even more challenging. One case in point of this is the California Online Privacy Protection Act 2002. Here we have legislation that goes beyond anything that the federal US government had at the time but has, alongside the EU Data Protection legislation, inspired the federal government to act. The resulting legislation includes the Notification to Risk to Personal Data Act 2005 and the Personal Data Privacy and Security Act 2005.

It would be wrong to assume that the legal conceptualisation of cyberspace is a 'top down' activity. Matters are far more complex than that. I have devised Figure 1 below to demonstrate who is involved in creating cyberlaw and thus is involved in the legal conceptualisation of cyberspace.

Figure 1: Parties to and structures of cyberlaw



The figure reflects the complexity of legislating cyberspace, it does not show the actual control structure of cyberspace – which I will discuss later on. I begin explicating the diagram by first looking at business and then private/public interest groups.

Reviewing the legal purposes of most cyberlaw the single most influential factor is that of business and economic growth. International bodies and governments – between each other, on national and local levels- have recognised the immense importance of cyberspace for their respective economies and thus legislate accordingly. This explains the powerful influence that business has on the legal conceptualisation of cyberspace. Therefore, the majority of cyberlaw deals with matters such as data protection, customer rights and privacy, business protection, business responsibilities, and regulating international disputes.

Furthermore, private and public organisations, using lobbying and media campaigns, are influential in two main ways. Firstly, they encourage the legal regulation of cyberspace on the basis of a need to control crime such as child abuse. One such example is the NSPCC. Secondly, there are private and public interest groups who try and influence the law in a way that protects the rights of the individual users to privacy, freedom of speech and confidentiality. One such group is the donor funded non-profit group the Electronic Frontier Foundation (EEF).

Last but not least there is a need to mention the media and politicians. I have not included them on the diagram itself because their overall impact is negligible. Drawing on Cohen's (2002) moral panic theory, in particular his idea of the media inventory, one can see that there are cases in which the media and individual politicians have been very influential in the debate about the need for stronger legislation of cyberspace. The classic examples of this are child abuse and cyber-terrorism. A politician tends to become the public spokesperson /sponsor of a bill through media or interest group lobbying. He or she puts forward a bill or a white paper and sometimes a cyberspace Act gets passed. However, once it is put forward the media and the initial politician, at least in the case of cyberlaw, tend to lose their control over the Act. Interestingly, public and private interest groups have managed to get Acts withdrawn because they contradicted other legislation or they infringed on individuals' rights. The most prominent example of this is the US Child Online Protection Act (1998). Therefore, while sometimes the media and individual politicians may set off a debate on cyberlaws they are relatively

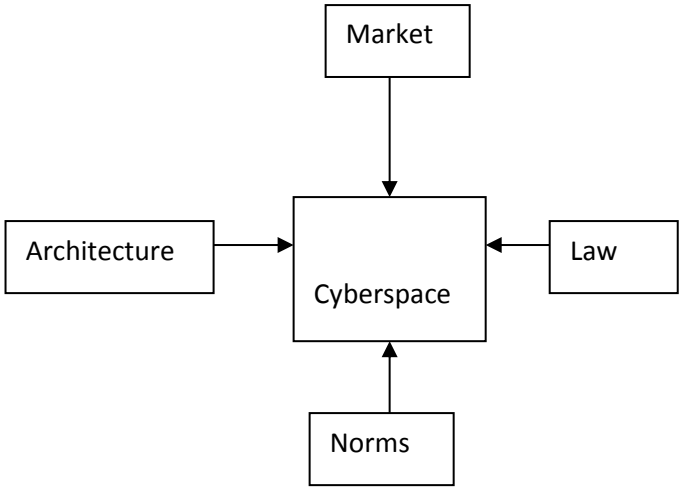
unimportant in the actual legal conceptualisation of cyberspace. Nonetheless, they are very influential in shaping public opinion of what cyberspace represents and how it should be regulated.

A final source of legislating cyberspace are the courts. In a way it is there that most of the conceptualisation and shaping of cyberspace takes place. Lessig points this out when he writes "They [the courts] were making, not finding, the nature of cyberspace, their decisions are in part responsible for what cyberspace will become" (Lessig, 1999:216). Over the period of time in which I wrote this thesis there are numerous examples where courts have changed the nature of the Internet and cyberspace through their decisions. It is important to remember that while this is the case there is no clear agreed upon basis but the decisions have led to a rather complex and at times contradictory understanding and form of cyberspace. The most recent example is the decision by a US court that Google has to reveal the viewing habits of YouTube users to US companies. This decision changes the privacy rights of Internet users, and crucially puts jurisdictions into question, changing the geographical nature of cyberspace.

4.3 How is cyberspace actually regulated?

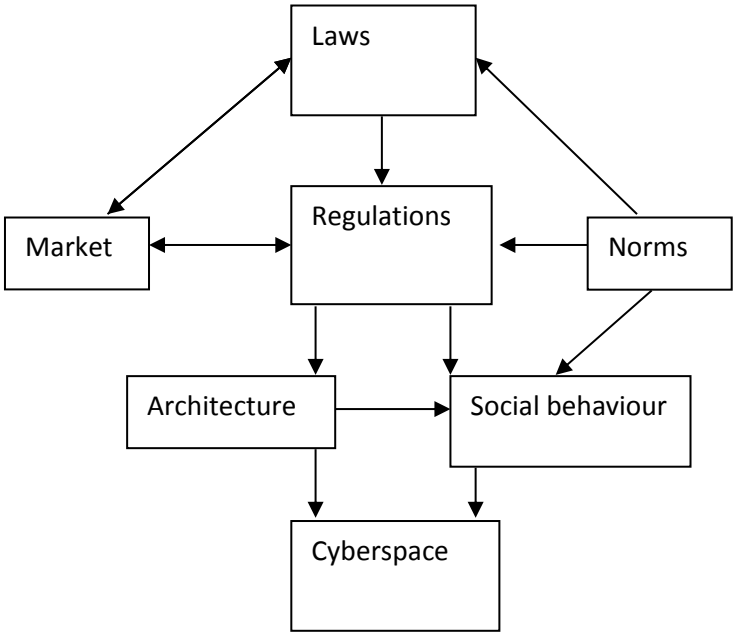
As I mentioned above, the legal conceptualisation of cyberspace is not the same as the actual regulation of it. Lessig (1999) suggests the following structure that regulates behaviour in cyberspace (see Figure 2).

Figure 2: Lessig's model (1999:88)



While this is a good starting point I would suggest a slightly altered figure (see Figure 3)

Figure 3: Proposed reconceptualisation



In this model cyberspace is currently regulated in the following way. Legislators produce legislation according to social norms and values, market needs and government responsibilities. These laws regulate the way in which the market functions online, the way Internet control institutions such as ICANN function, and the ways in which and the kinds of services Internet Service Providers (ISPs) offer to their users. Regulations by ISPs are influenced by legislation, regulation through specific institutions (ICANN), market forces and social norms and values. ISPs then create rules that regulate the code of cyberspace and thus its actual architecture. At the same time they regulate the social behaviours of its clients by telling them how to use and to appropriate the provided architecture and communication tools. The regulated appropriation and use of the architecture and communication tools then brings about the social sphere of interaction known as cyberspace.

4.4 Restricted creativity

The purpose of this chapter was to establish whether and how legislation and regulation define, create and shape cyberspace; and to conclude by beginning considering what this may mean for ethical guidance of online social research. I uncovered the ways in which cyberspace is legislated and regulated by outlining key developments of policy regarding the Internet and cyberspace; and illuminating the complex ways in which different relevant social groups come together to define, create and shape cyberspace.

The evidence provided in this chapter demonstrates that the Internet and cyberspace have always been legislated and regulated and are far from the utopian ideals of freedom and independence proclaimed by some authors and commentators. My analysis further shows that there is a tension between legislation and private regulation which is due to the uncertainty of governments whether they should actively control or take a more 'laissez-faire' attitude. Closer reflection on laws and regulations clearly shows that they actually create and shape the technology that is the Internet and the environment that is cyberspace. However, I suggest that any legal – regulatory conceptualisation of cyberspace is only ever a snap shot of that moment/ period in time. This is not because of the social interactions that the technology enables but because of the constantly evolving nature of legislation and regulation. Now that I have delineated the kind of cyberspace that emerges out of legislation and regulation I am able to begin reflecting on what this may mean for the ethical guidance of online social research.

First of all the evidence provided in this chapter means that current guidance is based on the incomplete understanding of what cyberspace is. This is because it is based on the ideas outlined in chapters two and three that conceptualise cyberspace outside of the legal and regulatory sphere and focus overly on social interactions and the use of technological tools. Doing so arrives at an entirely different ontology of cyberspace. As guidance is always constructed based on our understanding of the particular research context, a particular epistemology emerges. Continuing along those lines, one may argue that from this point of

view online social research may arguably be its own paradigm, with its own ontology and epistemology as long as it is understood as a parallel, separate world that is free of offline legislation and regulation.

However, this chapter clearly demonstrated the fact that cyberspace is constructed by laws and regulations. They are the foundation of what cyberspace is and only then can users appropriate the technologies and through social interaction create the social spaces that make up cyberspace. The ways in which they can and do interact are clearly set out through a legal-regulatory framework. Therefore, ethical guidance of online social research has to be based on a conceptualisation of cyberspace that has as its common starting point continuously updated understanding of the laws and regulations that shape this sphere of social interaction.

Seeing that current guidance of online social research is based on an incomplete understanding of cyberspace we have to question its worth. Putting it simplistically, the way we construct ethical guidance is by saying "under these circumstances, these ethical issues are likely to arise; do this to avoid them or if they do arise take this action to resolve them". In this case, where there is an obvious incomplete if not misinterpretation of the research environment, this approach may lead to several outcomes.

First, we may identify ethical issues that will not actually arise because we have misunderstood the circumstances of our research context. Second, we may not

identify ethical issues because we have not taken all the correct facets of our research context into account. Third, in this case were the law and regulations are so vital for the research environment not considering them may lead to ethical guidance that results in illegal actions. This is because we have not fully appreciated the potential legal and regulatory restrictions that are placed on this particular research environment.

Accepting that the law and regulations have such a profound role for and in this research environment, and the apparent lack of reflection on the issue, one may question in how far current ethical guidance is capable of responding to risk in this environment. Thus the legal and regulatory conceptualisations of cyberspace mean for online social research guidance that there is a need to:

1) Define cyberspace based on legal and regulatory realities merged with social theory conceptualisations of the Internet and cyberspace.
2) Use this 'new' conceptualisation of cyberspace to reflect on current online social research practice and the research environment to identify potential emerging risks.
3) Reflect in how far current ethics codes are able to manage these risks.

Chapter 5:

The impact of legislation and regulation on online social research

5.0 Introduction

Having established the significance of legislation and regulation in not only understanding but more importantly creating cyberspace, one has to consider their potential impact on social research that takes place in this specific environment. The main purpose of this chapter is to identify potential impacts of legislation and regulation on online social research in order to then use these as the basis to assess the adequacy of current ethical guidance in chapter six. To this end this chapter zooms in to focus on particular regulations and laws and critically reflects on their potential impact on online social research practice. By legislation I refer to the means by which the state directly regulates online service providers and interaction and thus the shape of the Internet and cyberspace. By regulation I refer to the ways in which Internet service providers respond to the legislation and their own economic objectives and shape the Internet and cyberspace in those ways.

5.1 Do we need a legal framework?

In current social research practice there is very little discussion about the legal aspects of research. The exceptions are areas such as researching children, vulnerable groups or research on medical topics. In general though, researchers

rarely reflect on any laws beyond the Data Protection Act 1998 and of late the Copyright Act 1988. There certainly is no public academic engagement with the issue in the mainstream. The places where researchers are made aware of the laws that are relevant to them tend to be within their code of conduct documents or as an aside on ethics guides. Several institutions, such as the University of Sheffield, have made a more concerted effort and produced a detailed breakdown of the Data Protection Act and what it means to social research practice. Their work was particularly informative to this chapter and I will draw on it later on. However, in my searches of the literature researchers do tend to focus more on being ethical rather than on being legal. There is arguably lack of serious engagement with Acts when it comes to which bits of an Act are and which bits are not adhered to. The key example for this are the arguments and activities by the proponents of covert social research.

I suggest that this ambiguous relationship between social researchers and the law stems in part from the fact that there is no law that specifically addresses social research in its provisions. Even the Data Protection Act, while referring to research, remains ambiguous what it means by this and most could rightly assume it to be about market research. The issue is that acts tend to state that they apply to business, journalists and artists, but where do the social researchers fit into this? In this context what entity is the social researcher?

The current situation suggests two things. Firstly, it suggests that laws do not apply to social researchers as they are not explicitly named. This interpretation

means that any incorporation of legislation into our overall ethical considerations is a bonus. However, it would be folly to suggest that social researchers work outside of the law. Indeed the establishing of research governance has made clear that certain laws and regulations do apply to social research. Secondly, the situation suggests that social researchers have to choose which category they fall into. I argue that to some extent this is the case. This is due to the nature of our activities. While many hold a somewhat romantic notion of what it means to be a social scientist (neutral, objective, searcher of truths for the better of society), the reality is rather different. We are not artists and certainly not journalists. I suggest that our research activities fall squarely into the domain of business, as defined in legislation. In most cases we 'sell' our services to interest groups, gather data, analyse it and produce a report that we hand over to our sponsors. In a sense our activities, while much more theoretically and academically grounded, practically are very similar to the methods of market research. The key difference may be the purpose for which research is carried out.

When taking this line of argument the logical consequence is to argue for the need of a deeper engagement with the law. There is a need to decide where legal considerations fit into the social research process, and the relationship between ethics and the law. This would result in two kinds of legal frameworks. Firstly, there is the internal legal framework that, similarly to ethics guidance, covers the essential legal basis for social research that has to be met. Secondly, there would be an external legal framework where existing and new legislation incorporates sections regulating social research. Regulating is not meant in a restrictive, but

rather a liberating sense. It can only become a liberating force, however, if we have a clear internal legal framework and draw on it to take an active role in shaping new and existing legislation, to ensure that social research can be carried out in an unambiguous and legally informed way.

When this is the case for social research in general, a sphere of social interaction that is shaped and created by laws and regulations –as seen in chapter four- consequently demands that we consider the question of whether we need an internal and external legal framework for online social research in order to strengthen current ethical guidance's ability to manage risk in online social research. This consideration is undertaken by demonstrating the current regulation and legislation of cyberspace in the key areas of data protection, privacy, surveillance and children and minors; and an analysis of what these mean for research activities of online social researchers.

5.2 Methodological foregrounding

It was argued in the previous chapter that cyberspace is created through legislation, regulation and code and that these three elements do so in integrate and complex ways. However, the discussion was kept quite general in order to get a sense of the legal conceptualisation of cyberspace. In this chapter, I zoom in, to consider specific regulations of cyberspace, particularly those regulations of tools that are most commonly appropriated by online social researchers. They are regulations of chatrooms, email, Instant Messengers (IMS), messaging boards, email groups, and online games. However, regulation goes deeper than what I

would consider front end or service tools regulation. There is critical regulation to be considered before one even uses those end user tools. They are data collection policies, privacy policies, and surveillance. These are critical as they frame the kind of end user tools that are available and how they may be used.

Therefore, the data for this chapter consists of 11 regulatory documents (see Appendix 1). They include such documents as the BT Privacy Policy (February, 2008), the Yahoo! Terms of Service (2004-2007), and the Tiscali Acceptable Use Policy (February, 2008). The key determinants of the sample were: the size of the ISP and thus the number of users it may impact on; how many other regulations a particular regulation had informed; and if there were any particular points raised within them that would have a particular impact on online social research. I have also included regulations from Keele University such as the Keele University: Policy on Monitoring and Interception (February 2008). I have done this as that was my home institution at the time and thus could serve as a vignette of the extra layer of regulation beyond that of ISPs that has an impact on online social research.

In terms of legislation my sample consists of 82 Acts (see Appendix 1). I have classed them under the following subcategories: Data Protection and Privacy laws; Security, Crime and Surveillance laws; Children laws; Technology laws; and Media Use laws. The legislation was drawn from a range of Western countries such as the US, UK, EU, Germany, and Australia. This is for three reasons: at the time of my study the majority of legislation on the Internet and cyberspace stems from these countries; I would argue that as a Western researcher using Western places

in cyberspace (e.g. US chatrooms, UK websites) with a sample dominated by Western research respondents this is the legislation most likely to be of relevance; there is a language barrier in that there may be relevant legislation in countries that have not been translated into a language that I do understand and thus cannot be included. Not all of the legislation that has been analysed is referred to in the text explicitly but forms the general backdrop to the argument presented in this chapter in particular and throughout the thesis in general. This is because of possible overlap between legislation and the fact that I had to focus on key issues to construct, test, support and illuminate my argument.

Both regulations and legislation were studied with a specific research schedule (see Appendix 3) in order to draw out key themes and to ensure a consistent approach of analysis. I chose to adopt the tool of a research schedule for similar reasons for which they are adopted in interviews or observational studies. As my 'subject' consisted of documents I adopted this tool because it offers a structured way of assessing a large number of different legislation by keeping the activity systematic and treating them with the same measuring tool. Beyond this it gives fellow researchers a clear insight into the way I have 'measured' and 'assessed' my data and allows them to test my findings by replicating my research. The initial schedule was piloted on 4 laws and 4 regulations and the resulting edited research schedule for legislation and regulation was based around 16 key questions which emerged in my engagement with the literature. The main aim was to learn about the aims of the legislation/ regulation; their purpose; their target audience; and then several questions that framed my reflections on their

potential impact on current online social research practice and its ethical framework.

5.2.1 Illuminating existing regulation

The general experience of the majority of Western Internet users is that they use their home or work PC to access the Internet. In both cases they have to accept and subsequently subscribe to certain rules in order to be granted access to the services they are intending to use. There are several 'layers' of regulation that the user has to conform to. There is the underlying layer of the Internet Service Provider (ISP) and then there are layers of employer's terms of use and layers of other service providers' regulations.

As mentioned above there are certain key regulations that need to be considered first – terms of service, data collection, privacy policies and surveillance. When signing up to the Internet the user has to accept the terms of use set out by the ISP. In this document the ISP makes clear the rights and responsibilities of the user and the ISP, and it is this document that is at the heart of the regulation of cyberspace.

The terms of service document tells the user what they are allowed to do, what they are not allowed to do, what the ISP does to user generated materials, what laws apply, what data is collected and what happens to that data. The latter two are only discussed briefly in these documents as each ISP also has a separate privacy policy.

An analysis of the Terms of service of key UK ISPs (Yahoo!, Tiscali, BT, and Sky) tells us that their regulations shape the Internet and cyberspace considerably. They do this by controlling: user activities; the services that are available to users; what happens to submissions; when services are available; age of users and the services accessible to them; (indirectly) the content of submissions.

ISPs control user generated message content in two ways, indirectly and directly. The direct form involves accessing messages and explicitly checking the content of that message. This occurs when the ISP is presented with a warrant from law enforcement agencies, but also when the ISP suspects that the content of a message may be breaking the terms of service agreement. The much more invasive means of regulation is by indirect control. The terms of use lay out very clear rules of what is not permissible as message content. The lists on prohibited content are very long. Most of the items are straight forward such as illegal material, criminal offence, abusive, unsolicited and harmful messages. Less clear are items such as 'otherwise objectionable' or 'likely to cause annoyance'. The difficulty is that there is no clear definition of what they mean by 'otherwise objectionable' or 'likely to cause annoyance' and who decides what is either objectionable or 'likely to cause annoyance'. As a researcher it is important to protect the integrity of our communications with our respondents. Thus, the potential question here is what to do when the integrity of our communication is in doubt. One may argue that the risk is very low and continue with the research while another may argue that the risk of interference posed by this set-up is too high and thus not undertake the research. The challenge in making the decision

is that we do not have clear definitions or 'case law' that may inform us on when we can and when we cannot assume security of our communication.

When it comes to the question of which laws apply to the ways in which users use the services, the majority of ISPs state that the first laws to be considered are those of the UK and the US. However, they also reflect the somewhat uneasy international legal status of cyberspace, by stating that the local laws and rules regarding online conduct and acceptable content where the user resides also apply.

The terms of use regulations set out by employers are very similar and mostly build upon the rules outlined by the ISPs. What is noticeable though is that employers add a second layer of regulations by further restricting the services available to their employees either by technological means or by rules. This means that while at work an employee may well be able to access the Internet in general, however, the employer may have very strict rules as to what is allowed to be looked at, for how long, or what kinds of emails are permitted to be sent and received.

The other key area, as mentioned above, is that of Privacy statements. These policy documents define private data, they outline what data is collected, when, how and why it is collected. They further establish how the data is used; who has access to it and for how long it is kept for. Last but not least they identify the laws that apply and users' rights. I outline these below.

Personal data is defined as "Information which identifies a user as an individual, or is capable of doing so" (BT). Thus personal data is often also termed personal identifiable data (PID). Internet service providers (ISP) then usually go on to provide a detailed list of what kind of data or combination thereof constitutes PID. The following list presents the most commonly collected personal data:

- Names
- Birth date
- Gender
- Post code
- Occupation
- Industry
- Personal interests, favourites, preferences
- IP address
- Pages requested / viewed
- Email address
- Home/ work address
- Credit card number
- Billing address
- Links clicked on
- Browser type and language
- Access times
- Referring website addresses
- Commercial transaction with or any third-party retailer
- Phone number used to dial into the Internet (Tiscali)

- Amount of time spent online
- Internet searches

This suggests that the user is readily identifiable. However, ISPs insist in their privacy statements that the individual is not identifiable. This is because the data gathered tends not be linked (i.e. only certain data is collected at certain times and not all the data all of the time). This implies that companies collect vast amounts of data that on their own are meaningless – which is doubtful. Such an approach stands in direct contrast to the reasons why these data are collected in the first place. It is correct that not all ISPs collect all of these data all the time; rather they collect them or combinations of them at varying times throughout the service use and depending on particular activities. Personal data are collected mostly for business, but also for security reasons. If users remained entirely unidentifiable, ISPs could not meet their own needs or comply with current legislation.

Further, their use of a technique known as data profiling also undermines the claim that users remain unidentifiable. Data profiling collects data on individual users and makes relevant connections with the aim to compose a matrix that represents a user. Companies like Facebook are pioneers in this area, but all other companies have followed suit. Also relevant here is to mention that data profiling occurs internally and externally. This means that companies seek not only to combine personal data of individual users within their own service provision but to also track their user activities while using other companies'

services. ISPs do not always have to do the external data profiling themselves but receive relevant data from third parties too.

To collect data in the first place or to gain more data, most use cookies – programs that are placed on one's computer when accessing certain sites or services that remember user settings and also track user activities. BT, for example, uses two types; a session based and a persistent cookie. Another popular tool is web beacons. These programs check whether an email has been read and which links within an email were clicked on.

All these activities outlined here show a well organised and far reaching, detailed routine collection of personal data. For how long data is kept varies widely and there is considerable overlap when it comes to general personal data. What is of particular interest is that companies tend to keep personal data on individual users even after that user has stopped using a company's services. Yahoo! states that user data may be kept, stored and used even after the deletion of a user account. Tiscali keeps updating information on the phone number used to dial into the Internet even after the termination of a contract. Facebook has been investigated in 2008 by the Information Commissioner's Office (ICO) because it keeps user profiles even after the user has deleted the account, which may be breaking current UK Data Protection legislation.

When it comes to how this personal data is used most companies state in their privacy statement that personal data serves to review services, monitor use,

internal analysis and research, and to communicate with users. Personal data will also be shared with third parties for service provision, and law enforcement. The documents appear to make clear that personal data is only accessed when required or permitted to do so by law. However, ISPs also appear to be less keen on being very specific about when and who accesses the data for what reason. Terms such as "when required", "if questionable" are not further defined and do not really illuminate the rationale by which companies justify certain actions with regards to personal data. When it comes to who has access rights to the personal data ISPs are similarly vague. The Keele University Computing and Information Systems Conditions of Use for example states:

> "staff maintaining and management operations have the right to access user material and monitor network traffic, but only if necessary to fulfil their role" (2002).

So who is that and why exactly? Yahoo! is also not very specific when stating that only 'key personnel' has access to personal data.

Data collection, storage, access and use are governed by legislation. Specifically the Data Protection Directives of the EU and individual member states and the so-called Safe Harbour Agreement are the basis for current ISP regulations. The data protection acts are the key basis from which ISPs have sought to develop their privacy statements. The Safe Harbour Agreement has been put in place by EU and US companies to ensure a high standard and mirror the EU Data Protection Directive in the US –who does not have a Data Protection Act like the EU – to

allow US companies who sign up to the agreement the collection, storage and use of personal data of EU citizens.

The final consideration in this section is that of users' rights. All privacy statements include a brief section on this and any close observer will note how limited the rights of users actually are. The user has the right to check what data is held on them, that the data is correct and can request that data is corrected where necessary. In some cases the user can also request that ISPs stop collecting data after the contract termination. One example of this is Tiscali's practice of collecting information on the phone number used to dial into the Internet. A real shortfall, however, is that the onus is on the user. For example, if a user wanted to find out what data and why it is held on her by BT, she would have to send a formal request and pay £10 to BT.

5.2.2 The impact of regulations on online social research practice

Having analysed how ISPs regulate the Internet in detail, I now identify several key areas within regulations put forward by Internet service providers that have a direct relevance and impact on online social research practice. In the following section I discuss those areas and their impact in detail. For the purpose of this discussion I group the areas under the following sub-headings: the practical dimension, researcher responsibilities, and monitoring / surveillance and confidentiality.

5.2.2.1 The practical dimension

ISP regulations have a direct impact on the nature and the longevity of data such as messages, emails, postings and personal data. At a very basic level ISPs do not guarantee that messages are passed on and do not take any responsibility for data loss of any kind. This means for social researchers that they cannot be certain whether their messages actually arrive nor can they feel confident that the content of the message is complete. Furthermore, researchers cannot necessarily trust in the safety of their email folders or online data bases. These two points have a real impact on the nature of the data that a researcher has to analyse and the kind of conclusions that he may draw from it. It may also pose ethical dilemmas. One example may be working with vulnerable groups where there is a need for sensitivity in communications. A break in communication caused by not receiving a response message or an incomplete message may be detrimental. I do acknowledge that I am identifying 'a worst case scenario'; however, as argued in Chapter one, I believe it is important that social researchers consider the potential impact carefully to then make informed decisions on their own current circumstances and research plans.

Another regulation that impacts on the data is that ISPs will delete files that exceed the limit of a user account. This again has practical implications for the social researcher in that it is quite possible that data is lost. While some loss may not be of importance; it is a matter that may impact the depth of information gathered. In an ideal situation social research data should be gathered until the researcher is satisfied that the relevant data has been collected, and not be based

on threshold set by an external party for entirely different reasons. Making this worse is that usually the ISP does not inform the account owner that he has not received messages. All they do is indicate, when logging into an email account, that the account is close to or at its storage limit. More worryingly is the policy to stop particular services at any moment of the ISP's choosing. This could mean that an online discussion group set up by the researcher may disappear 'overnight' undoing all the work carried out thus far.

The solution to this may well be to make use of university resources who tend to offer higher levels of over all data security enshrined in their service provision and terms of use statements; however, there are serious limitations with regards to functionality and availability of research tools and data storage. Using university systems also means being tied to a particular institution – which may want to influence the research in a specific way, often is marked by software conflicts and can be problematic in terms of data security due to locality and small numbers of servers.

A further issue is that even after the deactivation of an account some data may be kept by the service provider. This has real repercussions for the researcher as it can impact on the researcher, the research participants and others greatly. We may find that even after the conclusion of the research and the use of a service provider, the service provider may still hold partial or complete evidence of the research communication. In a worst case scenario the service provider may pass on this information to third parties who then take action against the researcher or

the research participant. Similarly, it is policy that online communications are archived. Again, even though the research communication has stopped, there is the future possibility of interaction with that communication leading to possible unwanted side effects. Some of them may include researchers and former research participants being contacted, their information being used against them or out of context. Again, this is raising some pertinent issues by using the worst case scenario. However, I defend this by reminding the reader that the purpose of this thesis is to test whether current ethical guidance is adequate in managing risk in online social research. Thus it is important to take into account these kinds of hypothetical research projects and outcomes as they identify situations in online social research that may go beyond standard ethical and legal guidance and considerations. My basic argument is that if we can manage risk in worst-case scenarios we can readily manage risk in more mundane every day online social research practice.

There are differing regulations that apply once messages are published. Some ISPs' regulations mean that once data is published via their service the published content can be used in any way seen fit by other users and the ISP as long as the use is within the law. This has several effects on online social research. First, it means that we could go online and cut and paste data – setting those social scientists free who wish to undertake quick covert research. While this is legal within those regulations, ethical researchers may feel uncomfortable with this approach. Furthermore, this set of regulations means that there are problematic consequences for our research activities too. If others can use our published data

(messages, postings, blogs etc.) for their own purposes, then how do we ensure that our communications are not taken out of context? How do we ensure that neither researcher nor respondent are harmed? How do we meet the ethical need of confidentiality? How do we protect anonymity? These are all very important questions that need to be addressed more rigorously than they currently are. I will employ these questions in chapter six to probe ethics guides under investigation. It will not be possible to discuss them in full within the aims of this thesis; however they remain an area ripe for future research.

In direct contrast to these regulations stand others such as those by Yahoo!. Yahoo! prohibits all extraction, collection, processing, combining or storing of personal data about their users or connected with their services. This certainly removes some of the problems identified above with the more liberal policies. However, it also puts into question any social research being carried out using Yahoo! services. Again, here is an example where past and current social research practice does not suffice. It is not enough to follow online ethical considerations and standard methodological guidance. Instead we have to uncover the regulations of our chosen medium or tool and once we have established that we are legally permitted do carry out certain research, return to standard social research procedures.

ISP regulations are also unclear about how they define SPAM. They are frequently not explicit enough and thus SPAM is often considered to be any unsolicited communication. This potentially means that research participants cannot be

contacted via email, or instant message, or posting to blogs and messaging boards advertising a research project; as this would represent an unsolicited communication. Instead potential respondents would have to contact the researcher first, consenting to and requesting to receive research communications.

5.2.2.2 Researcher responsibilities:

The ways in which data is collected, stored, used and regulated by ISPs has consequences for the responsibilities of a social researcher. In current social research those responsibilities are clearly defined through ethics guides and professional conduct documents. They include amongst other things protecting the interests of the research participant and preventing harm to the subject and researcher. So far that has been relatively straight forward and social researchers have usually been inventive in assuring meeting these aims. I argue here that this has been possible because thus far it was the social researcher who had access to and held, controlled and used the data. In the context of online social research this is not the case.

Ethical codes of practice consider it good practice to gain informed consent, which involves informing the potential research subject fully on the research project's purpose, which data will be collected, how it will be used and reported and what possible risks and consequences are. Now that ISPs collect the data of the respondents too, for very different reasons and purposes, is it the researchers' responsibility to inform subjects of their rights with regards to ISP regulations? Can the researcher and his participant possibly assess the potential risk and harm

in such a context where he has no control over how the data is collected, for how long, how it is stored and used and who has access to it? Similarly, while ISPs charge users to inform them about the data held on them, should the researcher pay this fee for the respondent? Further, as possible in some cases, should the researcher actively delete personal data held by ISPs during the research or after the research has finished? What about those respondents from countries that do not have a Data Protection Act or are not part of the/a Safe Harbour Agreement? The researcher would have even less control over how the data is gathered by ISPs and how it is used by whom for what purpose. Informed consent under such circumstances would be difficult if not even impossible. In some cases the researcher knows about 'internal' regulations of ISPs, however, sometimes ISPs use third parties to carry out work for them. The main ISP does not provide detailed information on the practices of that third party company, thus making traditional social research methodology even more problematic.

One of the prominent themes in online social research is that of identity or more specifically on the impact of cyberspace on identity creation and sustainment. Identity is also important in considerations in online social research methodology. ISPs require that users of their services provide true, accurate and up to date data when signing up to and using their services. This requirement poses problems for covert research in that the identity of the researcher is known. It may in some cases be possible to use a pseudonym in a chatroom; however, the true identity can be found out. This also poses questions for lurking practices preferred by some naturalist researchers. On the other hand these regulations mean that it

may be possible, in cooperation with the ISP, to check the accuracy of the identity claims by respondents.

One of the things that emerged in chapter three is the uncertainty over cyberspace being a free sphere of interaction. Chapter four showed that cyberspace is indeed less free than thought as it is very much created within legislation, regulation and code. The review and analysis of regulations shows that ISPs clearly frame the global within the local by tying their regulations and services and users to particular jurisdictions. Not surprisingly, the studied regulations give eminence to UK and US legislation. What did surprise me, however, was that ISPs tend to also identify the legislation of the country of residence of the user. It was unexpected as while the first laws help to clarify jurisdiction, rights and responsibilities; the inclusion of local legislation makes things very complex indeed. Thus a single chatroom can potentially represent hundreds of laws from around the world that are applicable to its interactions. This makes it easier for social researchers to begin considering the legal jurisdiction under which their activities fall. On the other hand, however, in a research environment where people of many different nationalities can be present, this can become very overwhelming. The issue are not the main laws from the UK, US and EU; rather difficult is to ascertain the legal framework from all the localities where data can be accessed and interacted with.

5.2.2.3 Monitoring/ surveillance and confidentiality

There are several regulations and thus resulting activities of ISPs and their third party sub-contractors that have an impact on confidentiality in the research process and in how far it can be achieved and guaranteed. I have already outlined those monitoring and surveillance techniques above and will thus focus on crucial elements to identify in which ways they impact considerations of online social research. For purpose of discussion I take the reader through each stage of data collection by the ISP during the research process.

In all cases of online social research the Internet service provider (ISP) actually collects data before the researcher even communicates with a potential respondent. Even if the researcher contacts potential research participants in the offline setting to conduct online research later on, ISPs still collect data first. In order to use a particular service a user has to register with an ISP. This means that at this point a whole range of personal identifiable data is collected. This data is not collected for the actual social research study. Thus, we have to ask what this means in terms of consent and confidentiality. Is it appropriate for us to ask respondents to give away personal details that are to be used in ways not entirely known to us? Our claims to guarding confidentiality are pretty futile in this context too. Do we have to gain their informed consent before asking them to sign up to a service that is purely about the service and not the research yet? From a legal point of view there is nothing wrong with ISPs collecting PID of our respondents. Yet, this practice represents ethical dilemmas – and is evidence for a tension between ethical and legal research.

A criticism of the argument that I present above may be that this is only an issue if ISPs actively observe the communication. That is a sensible point to raise; however, as I outlined earlier the researcher nor his participants know when communications may or may not be observed or analysed or passed on and for what purpose. Also, at this point I am interested in finding issues that may/ could arise in online social research projects that allow me to test the adequacy of ethical guidance for online social research in the following chapter.

The fact that personal identifiable data (PID) are not stored alongside each other (i.e. all the collected data on one person is stored in one file creating a complete profile) are undone as soon as companies employ data profiling and similar techniques. Again the researcher himself will not know exactly what information is actually held on his research participants. It gets even more confusing when taking into account that ISPs use third party companies, potentially resulting in a whole range of companies holding clusters of information that can easily be accessed and combined. Even this could be somewhat addressed if ISPs were to provide lists of third parties involved in the provision of services that the researcher is employing. What undoes this temporary reprieve is the fact that there is no publicly available list of the people who actually can access the data bases and the reasons for accessing those are vague as discussed above. While, I do not suggest that ISPs routinely or consciously link PID with research activities the routine processes outlined in this section are further evidence of my earlier assertion that normal social research procedures become problematic as soon as one considers Internet service regulations and strengthens the need for my asking

the question whether we need new and revised guidance for online social research.

Another thing ISPs do is access communications. Most of their policies state that this is not a routine undertaking. Nonetheless, there are various reasons why they may access this data or ask others to do so for them. They may access communication if they suspect criminal activities, harmful activities, otherwise objectionable activities or when presented with a tap and pen order or a subpoena. Of concern to the social researcher is the vagueness of terms such as 'objectionable'. Would it be objectionable to research young peoples' sexual activities in or via cyberspace? Would it be objectionable to discuss drug use or suicide? And as pointed out before, who decides on what is objectionable and what is this person's qualification to make such a decision? The academic literature does not address these questions and some of the traditional practice suggested by research guidance on for example studying sexual activities of young respondents may actually present contradictory or dangerous solutions. More important to me; however, is again the question of whether current social research guidance may offer us answers to these questions in a way that allows us to resolve these issues.

Furthermore, accessing communications can have several outcomes, all of which are not in the interest of the researcher or research respondent. Some possible outcomes are the deletion of messages or parts thereof, the misuse of the data for internal purposes and the handing over of data to law enforcement agencies.

This latter point means that some kinds of social research may not be carried out. What can happen was discussed in Chapter one using the example of the 'Nottingham Two'. Further examples include researching counter-cultures, illegal activities and resistance movements. How controversial this latter area is can be seen in the recent debates about Yahoo! and Microsoft passing on personal identifiable data of 'online protest bloggers' to the Chinese government (Karatzogianni, 2010). The communication by these bloggers was deemed as inappropriate and a threat to their national security by the Chinese government and thus the ISPs were required to reveal the PID of the bloggers. From a Western point of view the comments were not considered threatening (BBC News, 2005). While this is not an example of social research, one can see how easily research on the democratic movements in China via the Internet could have resulted in PID being requested by the Chinese government with unforeseeable consequences for the research subject. Therefore, one has to ask in how far we can defend using Internet tools when research communications could be quite easily spied on or misconstrued, taken out of context and used for entirely different purposes? Using university services as an alternative is not a solution here as their policies mirror commercial ISP regulations.

To some the last paragraphs may appear to suggest that it is preferential to hide the identity of respondents from official bodies. This is ethically speaking necessary in order to be able to fulfil traditional methodological objectives. However, here the researcher may find herself torn between ethics and the law. Legally, it would be the civic duty to pass on any knowledge of criminal or harmful

activities to the relevant authorities. This is not a new tension as criminologists in particular have had to contemplate this a lot; nevertheless, in the past when only the researcher collected the data she could be more circumspect in her collection of and recording of personal data (e.g. recording only demographic data and assigning pseudonyms or numbers to participants even during the research process) . Now that ISPs and other service providers collect the very same data and communications, the researcher has to reassess his position.

The final point of data collection to be discussed here is the ways data are treated by ISPs after the cessation of the service-user contract. Normally the data collection ends with the end of interviews and the return of questionnaires at a point of choosing of the researcher and his research participants. In cyberspace this is not this straight forward. Firstly, previous research studies have reported on a problem of the prolonged researcher-participant relationship due to the ease by which participants and researchers can stay in contact via the Internet. Secondly, and more importantly, regulations mean that ISPs may keep data after the deletion of the user account and in some cases even collect or pass on data to others much later on. This puts into question when the research ends and asks us to consider in how far we are responsible for the outcomes of continued data collection after our research project has been concluded.

5.3 The Law and online social research

The following section analyses legislation in the areas of data protection, privacy rights, children/minors, and surveillance to assess their possible impact on online

social research. Each area of legislation will be reviewed with the question in mind of whether the impact those laws may have on online social research warrants a call for legal guidelines for online social research.

5.3.1 Data Protection Acts

One of the key areas is that of Data Protection legislation. It is key for two reasons. First, because it is heavily drawn upon by academics when formulating research guidance. Second, it forms the basis of key regulations of Internet service providers and the ways in which they permit their services to be used by their clients.

After the analysis of Data Protection Acts at international, national and local level one of the things that stands out in relation to cyberspace is that this body of legislation does not define cyberspace. What these acts do is recognise that the social environment and means of collecting PID has changed considerably. Therefore, they point out that there is a need for new and or amended legislation. If this is the case then social researchers have to reconsider their ways of collecting PID too. Legislators have realised that in order for the Internet to develop further users need to trust that their PID and privacy are safe (see EU DPA Directive 1997; US Personal Data Privacy and Security Act 2005). In the case of social research this infers that if we want to instil trust in our research participants that their PID and privacy are protected and safe with us, we have to ensure that we adjust our online research activities accordingly. This, however,

can be very difficult to achieve in light of ISP regulations concerning their data collection and use policies outlined above.

PID or PII are usually defined to include an individual's last name in combination with any one or more of the following data elements: social security number, driver's licence number, account number, credit card number, passwords, passport number, telephone number, mother's maiden name, month, day and year of birth, racial or ethnic background, political opinion, membership of political association, religious beliefs philosophical beliefs, criminal record, sexual preference, health information, and an opinion (when ID is apparent or can reasonably be ascertained from the information or opinion). Of late new technological developments mean that this list is expanded by unique biometric data such as fingerprints; voice print, retina or iris image, and any other physical representation (see US Personal Data Privacy and Security Act 2005). This means that any data that normally tends to be collected by social researchers qualifies. The DPAs do not apply if the data is completely anonymised, however, this is virtually never the case as there are always ways in which subjects of online social research may be identified. The easiest way to do this is to identify the IP address as this is the unique numerical label given to a particular PC when accessing the internet.

Data Protection legislation sets out very clear conditions under which data may be collected. Part of these is that the subject has to be fully informed that their data is being collected, how it will be collected, what it will be used for, who has access to it, and how it will be stored prior to the commencement of data collection. This

means for the social researcher that he has to inform his potential subject about his intentions prior to collecting any data. This has immense implications not only for online social research but also for more traditional approaches such as participant observation. Be that as it may, one may state that academic endeavour is not the same as business activity and as the law does not explicitly apply to social research per se; researchers are exempt from this part of the law. Nonetheless, in the online context the researcher has to use tools that are provided by ISPs which are clearly subject to data protection legislation. Can we distinguish between the tool as a business service and as a research tool, which is independent of the former? Or do we have to, while applying the tool for very different reasons, still conform to the legislation that governs the code, regulation and service provision of the tool?

Furthermore, Data Protection law states that only those data that are relevant for that particular purpose – to answer a research question- may be collected (see UK DPA 1998; AUS Privacy Act 2005). This means that no extra data may be legally collected which led to an extended debate within the field (Corti, 2008). The outcome of this debate was the view that the DPA only applies to PID not to all of the research data that is collected. This may well resolve the matter of 'research' data. However, from the ISP regulations identified and analysed above we know that more data is actually being collected than necessary. Even though this extra data is not collected by the researcher directly, her activities make this further data collection possible in the first place. Which consequences does this have for the social researcher? Legally speaking, both levels and purposes of data

collection are, on their own, permissible. The question for us to pose is in how far it is ethically justifiable that this double data collection occurs? Further, we have to seek certainty that by our very activities caused further data collection is legal.

DPAs further state that the collection of data must not intrude to an unreasonable extent (see AUS Privacy Act 2005). What does the law mean by this? Judging by the negative reaction of some users to the 'intrusion' of their online place by social researchers, a cautious approach suggests to not use this research approach. However, there are at least as many positive experiences in this kind of scenario. The challenge is that there is no clarification on the following questions that arise when one considers the legislation. Is it the users' reaction that decides what is unreasonable intrusion? Could users use DPAs to take action against researchers on the grounds of invading their privacy unreasonably? When is that the case? These questions may well remain unanswered until they are tested in a court. Questions that arise that social scientists have to consider beyond this, however, is: Which procedures do we have to follow to avoid intruding unreasonably? ; and, do current guidelines provide an answer to this question?

The legislators do not just sit back and trust that service providers comply with legislation. In the case of data protection legislation they use software such as WebXM to identify whether websites that collect data include a link to a privacy statement. All websites that collect PID have to provide a link to the provider's privacy statement by law (see CAL OPPA 2004). If they fail to do so they face a fine and even the closure of the website. This has direct implications for all online

social research that uses websites as a portal to their research. In this case we have not just got the ethical but also the legal obligation to inform and to gain informed consent; and to do so by providing a clearly marked link to our research 'privacy statement'. The question that remains is whether tried and tested versions of the 'covering letter' are sufficient or whether we have to produce something more akin to professional/ business versions provided by the likes of Microsoft or Yahoo!. Currently, I was not able to unearth any legal guidance on this that addresses the special circumstances of social researchers.

Another matter that arises out of the current DPAs is to do with where the data can be transferred to geographically (see UK DPA 1998; EU DPA 2000). This is relevant to all kinds of social research. However, I would suggest, that in a multinational environment with multi-national jurisdictions, this becomes more problematic. First, the question arises of what is data transfer? There is the possibility of indirect or unintentional data transfer in online research when non-respondents happen to gain access to research communications in chatrooms or message boards. To what extend could this be considered data transfer? The other possibility is direct data transfer for secondary analysis and similar activities. This activity is limited in that the researcher has to gain informed consent in his initial data collection that includes the possible future use of data as secondary data. If there is any doubt, the law states clearly that data cannot be shared with third parties without consent. Beyond this, personal identifiable data of EU citizens is not to be passed on to countries unless they have an equivalent Data Protection Act or special arrangement such as the Safe Harbour Agreement (see

EU DPA 1998/2000). This part of the legislation prevents free dissemination of research data and one may argue could result in less comparative research and make the presentation of data and the checking of validity much more difficult.

An added area of interest on the subject of transfer of data is the right to request access to and to actively access PID by law enforcement agencies. Current legislation means that if there is threat to life, health or criminal activity ISPs may and in most cases have to share data. This has an impact on online social research in two ways. First, it poses the possibility that research data are passed on by ISPs. Second, social researchers have to reflect on when it is exactly that they have to –by law- share data with authorities.

Considering the first impact, it is particularly problematic that the ISP would share this data without the researcher's knowledge, thus making a risk assessment very difficult. Making things more complex is the fact that law enforcement and government agencies plus private organisations may also be looking at the communication and request the sharing of the data with them – again without the knowledge of the researcher and his participants. Examples may be research on or with under age respondents (Stern, 2002a; Holloway and Valentine, 2003), and sub-cultures (Armstrong, 2004; Arnold and Plymine, 2004; Douglas, 2004). In this light we have to reflect on the choice of tools, the methodological approach and our ethical considerations. It almost leads one to put into question in how far traditional research methodology and ethics can be upheld in a legal context where they cannot be realised and may even be considered illegal.

Thinking about the second impact one may use the example of researching suicide on and via the Internet. The particular example here is Stern (2004) who writes in detail about her ethical considerations on whether to tell 'someone' about her research subject's thoughts about suicide. In the end the research subject did commit suicide. My aim is not to judge the ethical merit of her actions; rather it is to show clearly that researchers have tried to resolve these issues previously by drawing on our codes of ethical practice. Therefore, while following her interpretation of ethical guidelines and codes of practice what the researcher failed to do was to consider the legislative framework within which she was acting. In this case the ethical conundrum would have been solved by knowledge of the law, which states that data ought to be shared if there is a credible threat to health (see AUS Privacy Act 2005; UK DPA 1998; EU DPA 2000). This is another illustration of the way that social research tends to rely much more on their ethical guidance and evidences a lack of knowledge of the legal framework within which their interactions online are situated. It also shows that current ethical guidance may not be able to manage risk in online social research properly.

Similar issues arise when researching groups that could be considered terrorists or organised criminals. DPAs state that data has to be shared with law enforcement in case of danger to national security or risk of crime. This is a part of the law that can be difficult to conform to by social researchers as they may use ethics to refuse to do so. Further complicating the matter is that not all groups are classed in the same way in all the countries that may have jurisdiction of the online space that we are using.

One example is that of Scientology. In Germany this organisation is classed illegal and considered a threat to the state. In the UK it is not. If one was to use online research this could very quickly lead to radically different obligations in terms of having to pass on data or not. Social researchers, it must be remembered, are citizens first and thus have to conform to their legal obligations first and their research ethics second. This last point is made explicit when law enforcement agencies present the researcher with a wiretap order or a subpoena forcing him to divulge PID (e.g. as in those referred to by Lee, 1993). Again, I am presenting a hypothetical case here as I am not aware of an actual case when this occurred. However, it is not my intention to only reflect on what has happened but on engaging with a wider reflection on the 'new' and 'different' research environment to identify what serious issues may arise in it and to then reflect on whether current research guidance is adequate to either prevent or resolve those situations. I also believe that this particular section of the act will have no impact on the majority of research; however, it can have considerable effects on research that is asking critical and important questions to do with terrorism, sub-cultures and political/ social movements.

There are some points where legislation and ethical guidance overlap. They are: that we have to provide a subject access to the collected data; we have to destroy the data if the subject requests us to do so; and we have to permit users to opt out of data collection. An apparent difference, however, is that the acts provide explicit guidance on within which timeframe this has to happen. For example data has to be corrected within 30 days. Furthermore, the Internet results in an ease

and speed with which online respondents can check and make requests in relation to their data. For social researchers this means that they have to manage their data bases much more actively than previously. Social research guidance is nondescript on this point and thus serves as further evidence that there is a knowledge gap and possibly a resultant gap in actual practice and practice guidance. This further strengthens the merit of a call for legal social research guidance.

One final aspect to consider is that DPAs do not permit businesses to send unsolicited advertising emails. Therefore, to send advertising emails they have to have prior consent from the recipients. If this is not the case the email will be considered SPAM, which will have serious legal repercussions. The question here is to what extent do emails 'advertising' our research to potential participants represent unsolicited email or SPAM. There is evidence in the literature (Williams and Robson, 2004; Bakardjieva et al., 2004) that Internet users, particularly those who use online messaging boards and chatrooms, have in the past regarded unsolicited approaches by researchers as offensive. Combining this understanding with present legislation puts some research practices into question. Again, there is no clear or agreed legal guidance for social researchers and thus it appears to be down to the individual researcher's interpretation of research governance, professional codes of practice, and ethical guidance as to how to resolve this important matter.

5.3.2 Children's Acts

Another key area is that of legislation covering the online activities of children and minors. Internet research involving children falls into several camps. There are those looking at children specifically and those who end up having children in their research sample due to their field of study (i.e. online gaming research etc.). Because of this and the large number of laws addressing online activities by children, it is important from a social research point of view to include legislation that targets children or the interaction with them to reflect on the question of whether we need legal guidance for online social research.

As with the above regulations and legislation I begin by considering in how far "Children's Acts" apply to social researchers. The list of Acts that were included in my analysis include the: Child Online Protection Act 1998 (US), Children's Online Privacy Protection Act 1998 (US), Dot Kids Implementation and Efficiency Act 2002 (US), Children's Internet Protection Act 2002 (US), Prosecution Remedies and Tools against the Exploitation of Children Today (PROTECT) Act 2002 and 2003 (US), Child Abduction Prevention Act 2003 (US), Jugendmedienschutz Staatsvertrag 2003 (GER), and the Deleting Online Predator Act 2006 (US).

None of the acts actually refers to social research and thus one may assume that our activities lie outside of their remit. However, when deconstructing who they are aimed at a different picture emerges. The acts are aimed at what is generally referred to as the 'operator'. The operator is considered to be the individual or company that provides a service aimed at and provided to children. These

services encompass websites, chatrooms, instant messaging tools and much more. In the case that a social researcher provides such a tool for children in order to carry out research, he would have to be considered an 'operator'. What remains uncertain is in how far making use of already existing tools would turn the researcher into an operator. For example, would someone using an online role playing game such as World of Warcraft be considered an operator when using the game as research space in which to carry out research by the means of participant observation? Also, in how far is asking questions or providing a questionnaire equal to providing a tool or a service to the child or minor? Again, I suggest these questions have to be decided by legal professionals as the term 'operator' is still to be interpreted and defined with regards to these questions.

Assuming that these Acts do apply I present the following arguments. Internet legislation on children and minors does not define cyberspace either. However, the introductory comments make clear that the Internet and cyberspace do represent a different sphere of social interaction. This sphere is understood to frustrate parental control and thus means that the state has to step in to fulfil its duty to protect (see US COPA 1998). In order to protect his own interests and to comply with the law a social researcher has to recognise that this is a time of change in law in a way that may well impact directly on their research practices. Therefore, there is a clear need to develop guidance on how to carry out legal online social research.

Similarly to DPAs this body of legislation insists on providing very clear information on websites regarding data collection (what, why, when, how, for what purpose and when it is disclosed to whom). Here it is important to establish in how far these bodies of legislation differ as it may be the case that subtle differences may require very different research practice responses.

These acts make clear that it is illegal to condition a child's participation in a game, offering a prize, or any other activity that encourages the child to disclose more information than reasonably necessary (see US COPPA 1998). When we apply this to social research it may mean that we are not allowed to reimburse our underage research subjects or undertake anything that may cause them to participate. Where do we draw the line? Can we still 'sell' our research to potential underage subjects to get them interested? One way of assessing the level of impact and thus the importance of these questions is by drawing on the work of Bosnjak and Batinic (2002) undertook a study to understand the willingness to participate in online surveys. Their research showed that

> "'Curiosity' was named as the most important motivational factor, followed by 'contribution to research', the appeal of 'self-knowledge', and last 'material incentives', ..." (Bosnjak and Batinic, 2002: 84).

This suggests that while the US COPPA 1998 does not allow the researcher to 'pay' for participation or to use 'payment' to bring about participation, in most cases researchers will not have to rely on this means as it is not the most important factor in determining whether individuals chose to participate in research or not.

Further questions that a reflection on this legislation raises are: what does 'not to disclose more information than reasonably necessary' mean? Can we really control this in an interview situation? What about asking deeper or follow on questions? Who decides on what is reasonably necessary? Is it the ethics committee that has to decide on how far we can collect data prior to carrying out the research? Again, as before, these are questions that inform my assessment of in how far current ethical guidance can provide answers.

Another area of this kind of legislation that needs analysis addresses the issue of parental consent. The default position in law is that for any kind of data to be collected from children the parents have to give their informed consent first. They have to be provided with information on what information is to be collected, when, for what reason, the use of the data, and the disclosure practices. Furthermore, the parent can stop the participation and data storage at any point in time. Also, parents are to be granted access to any data collected on their child. Accepting that these legal regulations apply to social researchers there are several matters of concern. First, having to gain prior parental consent is nothing new. It is consistent with tried and tested research practice and has only recently come into question as social theorists such as Lee (2005) and Alderson (2000) have placed more emphasis on the rights of children and wanting to make their voices heard. This latter position appears to be the default position in much online research.

The difficulty in the online context is that the only obvious way to gain access to the parent and to ask for their informed consent is by asking children for their parents' contact details. This, however, may already be considered an illegal activity as it would be understood as data collection without prior parental consent. There may be ways around it; nonetheless, the key point here is that there is a lack of guidance on how to proceed in the online environment. The law has, however, provided a solution in this case. The US Children's Online Privacy Protection Act (1998) states that if the data collected from children is only used to gain parental consent and is, when no consent is given, destroyed; then data collectors may ask children for PID of their parents prior to parental consent. The remaining issue is that this particular legislation is applicable to US citizens only. In terms of actual research I have not been able to identify any research accounts of how a researcher has dealt with this particular legislation or the issues brought about by it. The 'online' research with children has often been far closer to 'traditional' offline research practices (i.e. gaining access to children offline and then using the Internet as a research tool afterwards; or asking children or other gatekeepers for their informed consent rather than the parent). This is fine as long as it does not involve US citizens. The question for social researchers is how to negotiate this dilemma in other jurisdictional contexts in a multi-jurisdictional cyberspace environment.

Another ethical issue that arises due to the legislation is in how far it is justifiable that we share information with the parent. Personal data is defined slightly differently in the Children's Acts than in normal DPAs. The emphasis is on data

that permits the identification of children/minors online or offline. Personal opinions are not included in the list of PID presented in the legislation. Does this mean that researchers could collect data/ information on children's and minor's opinions without prior parental consent? Would we be required to grant parents access to this kind of data? Would it be sufficient to grant them access to the data that is considered personal identifiable data? Some of these questions could be answered by suggesting anonymising the data. That way PID is removed from the data set and what we are left collecting are 'opinions'. However, the latter question of whether and what kind of access we would have to give to parents remains to be decided. It is not a 'new' issue as this is true for 'offline' research with children too and thus one may draw on existing ethical solutions to this question while reflecting in how far these are in line with current legislation.

Furthermore, even though opinions on their own could be quoted by social researchers in their reports; the fact that these can be searched for and found and then linked with other communication data and PID suggests that reporting may be complicated. This is particularly important, as the law requires data collectors to establish and maintain reasonable procedures to protect the confidentiality, security and integrity of PII/PID.

There is one incident when there is no need for parent consent. If the Commission determines that it is appropriate to forgo parental consent, taking into consideration the benefits to the child of access to information and services and risks to the security and privacy of the child (US COPPA 1998). This is

problematic. Does it mean that if our research was on sexual health, or emotional issues, or other personal matters we need not worry about parental consent? This question presents considerable ethical questions/ considerations. The challenge in answering it is that the researcher, ethics committee, professional body has to successfully combine ethical considerations with the given legislative framework. This may well mean having to adjust the ethical answers/ responses to fit with the legislative framework.

The analysis of current legislation makes abundantly clear that past approaches that allowed for consent by gatekeepers do not hold merit any longer. They may still be appropriate in an offline setting, however, online, this is not the case. None of the legislation that addresses online data collection from children mentions a provision for gate keepers as a possible source of consent. Also, from an ethical point of view we would have to ask ourselves whether we can justify accepting informed consent on behalf of children from operators who may be underage themselves, do not know the potential respondents, or may not be accepted by potential respondents. Again, I will draw on these issues in chapter five; however, widely accepted current practice of using gatekeepers is clearly put into question by the legal reality of the online context.

A final area of legislation that focuses on children's and minors' online activities is that of sexual abuse or the sexual exploitation of them. This area has been subject to intense media interest and the legislation and practice of police and private and voluntary organisations are very important. They are very important

as they pose real concerns for social research activity. First of all it is illegal to search for, access, or download child pornography. It does not matter who one is or for what reasons one interacts with such materials; unless they are an officially authorized person, if found out, one will end up on the sex offenders register. If this is the case, then how can we pursue social research in the area of child abuse? The topic of online child abuse is of particular interest as it appears that these illegal activities have moved into cyberspace and thus offer new ways of research engagement. Would it be possible to research this topic with special permissions based around an agreement to pass on PID of criminals? How would this effect our ethical considerations and justifications?

Another issue that arises out of this body of legislation is the question at which point our activity crosses the boundaries between serious researcher and paedophile? Current legislation is not very specific and surveillance activities mean that any communication around sensitive topics may be observed or reported, even though they may not be undertaken with a criminal intent. I draw on the example of the topic of sexual health. What would happen if we approached under age respondents online in a chatroom and asked them to talk to us about their sexual health? Ignoring issues around parental consent, could we be reported and found guilty of entering into communications that are considered sexually offensive? This is yet another illustration of the current lack of legal guidance.

5.3.3 Surveillance

The final body of legislation to be analysed in terms of its possible impact on online social research is that addressing surveillance and law enforcement. Since the mid-1990s and particularly since 2000 there are a growing number of laws that address the conduct of law enforcement and Internet service provider activities in cyberspace. The reasons for this increase are: to account for technological change such as the growth of the Internet and strong encryption, to put other techniques of monitoring citizens on a statutory footing, requiring ISPs to put systems in place that allow the surveillance of users, to protect national security from erosion through technological change, to maintain the ability to intersect, and to directly respond to the terrorist attacks of 9/11. Examples of such laws are the US Communications Assistance for Law Enforcement Act 1994, the UK Regulation of Investigatory Powers Act 2000, the US Patriot Act 2001, NZ Telecommunications/ interception Capability Act 2002, GER Telekommunikationsueberwachungsverordnung 2002, and the CAN The Modernisation of investigative techniques Act 2005.

These and other Acts like them legislate and regulate the ways in which law enforcement agencies and ISPs can survey online activities of Internet users. Normally, law enforcement agencies have to get a court order or in the case of the UK receive permission by the Secretary of State, to be allowed the interception of data. The US Patriot Act of 2001, however, alters this. Law enforcement agencies or those charged with national security no longer need a tap order, a 'simple' search warrant is sufficient. Furthermore, the act permits ISPs to actively

intercept user generated data to protect their own interests. The interception of data is granted on grounds such as national security, protecting public health, preventing or detecting crime, preventing disorder, public safety, or in the interest of the economic well-being of the UK, to collect 'taxes', and in an emergency to prevent death, injury or damage to a person's physical or mental health. Furthermore, ISPs have to provide access to data and must not tell the subject under surveillance about it.

One illustration of how these agencies intercept data is the use by German inland security services (BND) of email surveillance at two points – at the level of the email system/ server and on the Internet using a SINA box. A SINA box does not observe individual accounts nor the targets of this account. It automatically takes snapshots of the entire communications targeted to foreign countries. The relevant information is then extracted by the BND by use of technologies such as ECHELON or CARNIVORE (Heise Online, 2007).

A further way to survey the Internet is by use of 'honey traps' (admissible in court). A more recent approach by police is to pose as minors or children in chatrooms, bating possible offenders to interact with them and attempting to investigate and possibly arrest them in the short term (BBC NEWS, 2006). Further to this, many child protection groups (ChildNet International, Cyberangels, ECPAT) actively survey the Internet and cyberspace social interaction and readily pass on information on online activities that they judge suspicious, dangerous, and inappropriate to law enforcement agencies. These groups follow their own

understanding of what is inappropriate or dangerous, that is based in law, yet heavily informed by their own moral values. Connecting this with the fact that ISPs and legislators do not clearly define what they mean by 'objectionable' this means that social scientists will have to include this in their ethical considerations. This is important as it is no longer 'just' important to judge whether a particular research subject would find a topic or question 'objectionable' but whether other interest groups which may have access to the communication would.

There are limits to surveillance too. The US Electronic Communications Act 1986 does discourage interception and considers a possible subsequent publication of intercepted communications as even more questionable. The UK RIPA Act 2000 makes it illegal to intercept communication in the course of transmission. This is mirrored by the US Patriot Act 2001 which makes it not only illegal to intercept communications but also, to disclose it. There are two exceptions to this. First, when the communication is readily accessible to the general public; second, when the officer is party to the communication itself; third – in the case of the German TKUV 2002- when the email server system lies outside of Germany.

What muddies the waters slightly is the US Online Freedom of Speech Act 2006, which states that one of its purposes is to "amend the Federal Election Campaign Act of 1971 to exclude communications over the Internet from the definition of public communication". This puts into question in how far we can consider communication that is readily accessible to the public as public communication. This latter Act suggests that even readily accessible communication is private.

The US Data Mining Moratorium Act 2003 goes even further. This Act draws the conclusion that the total information awareness program of the US government agencies was unsuccessful. It even judged it to adversely affect privacy and other rights of users. Therefore, the Act disallows the Department of Defence and Homeland Security data mining.

The length for which data can be stored varies greatly. The EU and member states regulations mean that data can be stored for up to 12 months (even though this is currently under review and many member states and regional governments decided on different lengths of time). The German TKUV 2002 aims to establish that data can be stored indefinitely. There are rather different approaches regarding who is granted access to information that is gathered in such a way. For example the UK RIPA Act 2000 adds extensions that mean that from then on jobcentres, local councils, and chief inspectors of schools have access to the surveillance data. In Germany the main groups with access are the police and the BND.

The analysis of these laws in terms of their possible impact on online social research illuminates several areas of concern. First, it evidences and further reinforces earlier claims that there is a threat to confidentiality in that the social researcher does not know when or why or how research communications may be intercepted. Second, those carrying out the surveillance may actually hold more information on our research subject than we do. For example, as users have multiple presences online, most of which are not known to the researchers, it may

well be that law enforcement agencies are made aware of the user through our research communications and then data mine further information from these other presences. Third, the research subject would not know when they are under surveillance. Normally we would have to protect their interests. How can we do that in this climate?

Fourth, recent legislation suggests that there is a drive to limit surveillance not per se but restrict the number of groups or individuals who can carry it out. Does this mean that we and our subjects can make better informed decisions regarding possible risks of surveillance? Should social researchers use this current climate to make their own needs heard and attempt to influence which groups can survey? Fifth, is our research communication public or private when using messaging boards or chatrooms? This is important in assessing which research tools we can use safely, how we can protect our subjects and our data, and whether agencies have the right to 'listen in'. Sixth, when do certain groups have access to the data and what are they likely to do with it? Again we have to ask this question with confidentiality, anonymity and risk in mind.

Seventh, how do we respond to foreign surveillance? One example of why we have to ask this is online gambling. US customs arrested non-citizens during a stopover after collecting evidence on them for running non-us yet accessible to US users gambling websites. This means that we have to go beyond protecting the interests of our respondents in their country of residence and consider how their research participation may impact on their standing in other countries too. Eighth,

how does the length for which data can be stored impact on the social research process? Could law enforcement agencies use stored data in the long-term like puzzle pieces to form a case against a respondent? What does it mean to social researchers to possibly produce communication data that may become part of a prosecution case (possibly even in a different country)?

Ninth, how do we respond to some of the more direct surveying approaches? How do we protect ourselves from being mistakenly caught in a 'honey trap'? How do we ascertain that our communications are not taken out of context by interest groups, who pursue very different goals in their data collection from us? Tenth, how can we make sense of the multitude of national laws, which often reinforce and contradict each other at the same time? Eleventh, how do we respond to a rapidly changing legal and thus policing environment?

When analysing the impact of this body of legislation on online social research it becomes obvious that this body of legislation has an indirect effect. By this I mean that social researchers do not have to comply with these laws themselves. Rather these laws apply to other individuals or groups who may want to carry out surveillance on us or our research participants. The major issues outlined above are those of confidentiality, anonymity and protecting the interests of our research participant in an environment that enables others to easily access essentially private research communications. It is the knowledge of these laws that enables us to better meet our ethical and legal obligations to ourselves, research participants, discipline, and our government. At the time of writing I was not able

to find another piece of work that engages with these laws in detail to determine how they may impact on online social research. Due to the outlined effects of the legislation there is a real need for considering how to respond to the arising issues sociologically and methodologically.

5.4 Lacking legal and regulatory insight

The purpose of this chapter was to identify relevant legislation and regulation on cyberspace and the Internet and to consider what questions they pose to current online social researchers, in particular with view to ethical considerations and guidance. To achieve this, the first half of the chapter unearthed the key ways in which the Internet and cyberspace are regulated by Internet Service Providers and then critically evaluated their impact on current online social research practice. The second half of the chapter illuminated three key areas of legislation (Data Protection, Children and Surveillance) and how they shape especially social interaction in cyberspace. Using this information I critically evaluated how this body of legislation impacts on current online social research practice.

The analysis of regulations showed that Internet Service Providers play a key role in shaping online social interaction, impacting on every element of it. Furthermore, I was able to demonstrate that the ways in which ISPs regulate their service use, poses many questions to online social scientists, particularly to their methodological and ethical practices. This is because regulations either force the users of ISP services to act in certain ways or permit the ISPs themselves to take several actions, which were shown to be problematic for social research. In many

cases this may mean that online social research is either prevented from using 'tried and tested' methods; that it may not be possible to meet ethical guidelines, or that research may not be carried out at all. Further to this, I showed that there is a need for, yet a lack of guidance on those regulations and how to resolve the resulting issues available to social researchers.

The analysis of key bodies of legislation showed that they also have a considerable impact on online social research practice. This impact is expressed most clearly through the identifiable tension between the law and 'traditional' and current methodological and ethical practice. In one way this tension was shown to be played out is through the choice that a researcher has to apparently make in this legal context between being legal or ethical. This is because current legislation (and subsequent regulation) may at times undermine, bypasses, and thus make it almost impossible to fulfil our ethical objectives or methodological practice in the ways we are used to. Furthermore, this section showed that there is a distinct lack of legal guidance available to social researchers that indicates how to resolve the issues that I have identified.

To conclude, it is possible for me to state that the discussed legislation and regulations have a considerable relevance for and potential impact on online social research, especially in terms of its methodological and ethical practice and guidance. Therefore, the lack of guidance on which legislation and regulations apply and the lack of clarity within laws and regulations on their applicability to online social research mean that online social researchers are faced with many

questions and dilemmas posing risks that current ethical guidance may not manage well.

The evidence in this chapter suggests that we do need to consider how we as online social researchers incorporate legislation and regulation much more explicitly in our research guidance and practices than we may have been doing thus far. The key outcome of this chapter is that it identified the questions and issues that we need to use as testing tools of current professional, particularly ethical guidance, to see whether it can be relied upon for guidance on how to resolve those issues successfully in order to manage the identified risks in the online research environment. If it does then we will not need a 'new' or 'different' legally framed ethical guidance. If it, however, does not; then the field will have to continuously review legislation, regulation and ethical practice and triangulate them in order to ensure good online social research.

Chapter 6:

Ethics and Online Social Research

6.0 Introduction

The previous chapter has shown that legislation and regulations have a considerable impact on online social research. I suggested, however, that this impact does not manifest itself in our being faced with new ethical dilemmas; rather, ethical issues are occurring in ways that potentially put into question our 'traditional' ways of addressing them. Thus, one has to ask whether current ethical guidance available to social researchers reflects this 'dilemma'; whether they provide us with adequate guidelines on how to carry out online social research in this legally shaped environment; and whether we need new ethics guides in order for our research practice to remain ethical and legal.

At the heart of our ethical practice lies our understanding of ethics given expression in and through ethics guides and professional codes of conduct. Arguably, these are the documents that inform every piece of social research that is carried out. Therefore, one can use them to investigate the central questions first identified in chapter five by undertaking a detailed analysis of current ethics guides and professional codes of practice. This chapter is divided into two main sections. The first section analyses current ethical guidance, comparing and contrasting general and online specific ethics guides. The second section deals

with the ability of those ethics guides to address and resolve the key implications current legislation and regulations have for online social research.

6.1 Methodological foregrounding

The purpose of this chapter is to establish whether current ethical guidance available to social researchers is adequate in managing risk of online social research by guiding and informing online social research or whether there is a need for new ethical guidance. To do this I have analysed 31 ethics guides and codes of conduct of key professional associations, governments and private organisations, universities, and Internet or online research specific ethics guides (see Appendix 2). I have categorised them under the following sub-headings: government and private organisations; professional associations; universities; and exclusive online social research ethics guidance. The criteria that I have applied to identify an appropriate sample are:

- Number of times guidance or code of practice has been referred to in the methods/ethics literature of this field
- Number of times guidance or code of practice has been referred to in research accounts on online social research
- The level of online social research activity at a particular institution

Therefore, the sample consists of guidance and codes of practice that have arguably had the widest impact as the majority of research practice that I have engaged with has been informed by it. Potentially, it will continue to do so because 'new' generations of researchers will, while doing the literature review for

their own projects, come across these and very likely adopt them as at least a starting point to inform their own research practice. Not all of the ethical guidance and codes of practice that has been analysed is referred to in the text directly but they form the general backdrop to the argument presented in this chapter in particular and throughout the thesis in general. This is because of considerable overlap between them and the fact that I had to focus on key issues to construct, test, support and illuminate my argument.

To analyse the guidance I used a specific research schedule (see Appendix 3) in order to draw out key themes and to ensure a consistent and systematic approach of analysis. This method proved valuable for the analysis of legislation and regulation. Hence, I created a schedule consisting of 23 questions; most of them where to elicit their purpose, but others were about guiding my reflection and allowing comparisons between them. After piloting the initial schedule on four ethics guides I applied the edited version to the 31 guides.

6.2 Ethical guidance and Online Social Research

In this section of the chapter I begin addressing the question of whether current ethical guidance can manage online risk by comparing different categories of ethics guides (Professional Associations, Governments and Private Organisations, Universities) to specific online social research ethics guides. The rationale for this approach is to establish how far these guides overlap, whether they deal with different ethical issues, offer different approaches and solutions; and thus justify

the call for either specific ethics guides for online social research or 'up-dated' new general ethics guides.

6.2.1 Examining emerging cyber ethics

To begin with I investigated whether the ethical guidance itself offered any comment on the need for new ethics guides. At this stage it was not of interest to check how far those claims could be substantiated. What it was to reveal were the underlying assumptions of those who produced the ethics guides and thus by default shape overall research practice.

Reviewing the general ethics codes it was of interest to note that the majority of codes do not refer to Internet or online research at all. They address a wide range of research environments and often make explicit reference to particular settings and their associated special considerations. The key example here is research with vulnerable groups, especially children. Overall, however, it is as if online social research was either not considered or thought to be sufficiently similar to more 'traditional' research environments as not to require special mention. An indication that the former is the case may be the fact that only two of the universities from my sample (the Universities of Sheffield and New Hampshire) have produced ethical guidance that either extended their former ethics guide and or produced separate ethical guidance for online social research. Thus, there is recognition of a difference and newness of the research environment that is not present in any of the other guides. Apart from this I was

not able to illuminate any other data that would explain why my sample's ethics guides had not addressed online social research.

Most insightful are those ethics guides in my sample that specifically address online social research. This is because they are explicit on two points: a) their justification for being and; b) their explanation of how far online ethical issues differ from offline ones. Here, I focus on their raison d'être while considering point b) later on in this chapter. Out of the six online social research ethics guides that I was able to identify, four argued that there is a clear need and justification for new, different and specific ethics guides that address the realities of online social research. The extent to which these ethics guides have to differ ranges from simply extending existing ethics codes to a call for the creation of entirely new and radically different ways of ethical practice. However, a closer observation of the actual guidance that follows those claims reveals a much softer stance than first expected.

Examples of these positions are the codes produced by The National Committee for Research Ethics in Science and Technology NENT (2003) and the Association of Internet Researchers AoIR (2002). NENT argues that online ethics do not differ from offline ethics as "Internet research is subject to the same ethical demands as other research" (NENT, 2003). The AoIR on the other hand justifies the need for new ethical guidance by pointing out that due to the interdisciplinary nature of online research, the large variation between ethics codes poses a central ethical difficulty for online social research. The University of Sheffield tries to reflect on

how far 'traditional' ethical issues are relevant to the online world, and moves towards online ethics in that way. This University first produced guidance on online social research by extending its existing ethics code in 2003 as it was felt that there were aspects of traditional ethics guides that can be applied. However, this approach appears not to have been sufficient as by 2005 the institution had developed a separate guidance "The Internet: Accessing Human Participants and or Data".

Overall, the majority appears to state that there may not be a need for separate ethics guidance for online social research, just an extension or a 'shift in focus' (University of New Hampshire). What does sit uncomfortable is that even though this is the message, apart from one attempt [University of Sheffield], all of the other online research guides that I was able to identify, have been developed as standalone ethics guides. At this point one has to move on to consider these ethics codes on a deeper level. What are their purposes, approaches and motivations?

6.2.2 Purposes, approaches and motivations

So far it is not clear whether current ethical guidance can manage risk in online research effectively or whether we need new guidance. What we have is a claim that there is a need for new ethics codes put forward in several 'stand-alone' online research ethics codes while the majority of 'general' guides are silent on the issue. At this point I therefore focus on the purposes, approaches and motivations of my sample. I do this to discern whether there is a marked difference. My line

of argument is that if there is a considerable overlap between the stated purposes, approaches and motivations between 'offline' and 'online' research ethics codes then the 'new' in new ethics codes may or could be limited to creating ethical guidance that extends existing guides. However, if their ontological and epistemological starting points are radically different, then the 'new' would mean separate, stand-alone ethics guides for online social research.

The overall approach of 'general' ethics guides in my sample to ethics can be summarised in the key concepts of non-maleficence, beneficence, and the principles of justice and fair treatment. The University of Sheffield provides a definition of ethics that is representative of the implicit understanding that I found throughout the 'general' ethics guidance. They state that: "The concept of research ethics marries the idea of undertaking original investigations in order to gain knowledge and understanding with the idea that such investigation must be undertaken in accordance with moral principles and values of right or good behaviour in relation to others" (University of Sheffield, 2003). Online research ethics codes share this basic starting point. However, due to the multidisciplinary nature of research in cyberspace, the multicultural nature of cyberspace and the large number of competing conceptualisations of cyberspace itself there is evidence of an approach to ethics that is not so evident in 'general' codes. This approach is a direct response to the resulting uncertainty and is expressed in online research ethics codes through attempting to achieve a position that is described as "a middle-ground between ethical relativism and ethical dogmatism informed by cross-cultural awareness" (AoIR, 2002).

I do not believe that this is solely a development in online research ethics thinking. There is plenty of evidence of this approach to thinking about ethics in mainstream ethics literature too. However, at this point my impression is that current 'general' ethical guidance has not been re-written to incorporate these developments (yet). Thus, the apparent advancement through online research ethics guidance may well – in part - be due to the fact that these guides have been written after these debates have become dominant in the mainstream. Therefore, at this point one may justifiably think that if there is a need for new ethics guidance then it may come in form of up-dated and extended ethics codes.

The analysis further showed that 'general' ethics guides are often written taking other existing guidance into account. The key features here are a combination of structure, the type of ethical considerations identified and their resolution offered. For example Lancaster University (2007) bases its ethics code on those of the Association of Social Anthropology, the British Association for Applied Linguistics, the British Educational Research Association, the British Psychological Association, and the British Sociological Association. The British Sociological Association (BSA, 2002 + 2004) itself acknowledges the adoption of other ethics codes such as those of the Social Research Association, the American Sociological Association, and the Association of Social Anthropologists of the UK and the Commonwealth. The reasons for adopting a particular ethics code for the creation of their own code are not given by any of the 31 guides that were analysed. Even though there is this element of eclecticism one can discern a certain hierarchy. By this I

mean that universities draw on other universities and professional associations and government guidance; and professional associations draw on other professional associations and government guidance.

At the moment there is an attempt to create a coherent overarching ethical framework for socio-economic research in the European context resulting in the project called RESPECT: professional and ethical codes for socio-economic research in the information society (2004). However, this code is itself a synthesis of a large number of ethics codes and EU legal requirements. Currently, due to their wide and explicit application, the most influential source of ethical guidance is guidance provided by professional associations. This is evidenced in (a) professional associations demanding that their members comply with their guidance first and (b) universities stating that their own codes are over-written by those of professional associations. An example of the former is the following statement: "… each sociologist supplements but does not violate, the standards outlined in this code of ethics" (International Sociological Association, 2001). Examples of (b) are the codes of Goldsmith College London, University of York and Kings College London.

When considering online social research ethics guides several similarities and differences to those above can be identified. Of the six online specific ethics codes three are those of professional associations (Association of Internet Researchers, American Association for the Advancement of Science, and the National Committee for Research Ethics in Science and Technology). However,

none of these associations has drawn on either the guidance of offline or online targeted ethics codes put forward by other professional associations, governments or private research organisations. Most notably of all are the instruction by the AoIR that researchers should turn to their own specific subject's guidance first and the lack of consideration of other online specific associations. At the level below, one can see more similarity in that universities draw on the ethical guidance produced by the AoIR; however, they do not adopt the codes of other universities. The example of the AoIR encouraging its members to refer to their subject's specific guidance first, gives further credence to the call for 'new' – meaning extended ethical guidance that incorporates considerations of online research.

Moving on to reflect on the purpose of the sample's ethical guidance one can state that 'general' ethics codes, while ranging from specific research focus to larger more far-reaching projects, share common purposes. They are to: provide high ethical standards; protect researchers and subjects; respond to external expectations; raise ethical awareness; spread good practice; and to address specific issues that arise out of studying specific groups (mostly children). They aimed to do this at varying levels of reach; some are aimed at a small number of academics at a particular institution or organisation while others are aimed at the whole of socio-economic research in the EU. The purposes of online social research specific ethics codes mirror those outlined above. The only additions are the purposes of contributing to the reflection, debate, and education regarding Internet research ethics and to encourage the study of known phenomena in new ways (NENT, 2003).

As a final point of consideration I studied the actual style of guidance. In the 'general' ethics codes, guidance was provided in one of two ways either very prescriptive or more aspirational in nature. This is also the case for online social research ethics codes. An interesting new approach is offered by the AoIR who instead of giving guidance per se, offers a list of questions that are to be considered before carrying out research. This is a significant departure from the "if a) is the case, proceed like this" approach favoured by most ethics guides surveyed and provides an interesting premise for the possible shape that 'new' or extended ethical guidance for social research may take.

Based on my discussion so far it appears that when considering the claims about, purposes of, approaches to and chosen execution of general and online research specific ethics codes one can confidently assert that there is sufficient common ground and overlap of the two camps that the 'new' in new ethics guidance means an up-dating and extending of existing ethics codes rather than the creation of entirely separate and different/distinct ethical guidance. This means that current ethical guidance may well be able to manage risk in online social research, but benefits from being extended to reflect potential amplification of known ethical issues and thus risks in the online research environment.

6.2.3 Ethical issues and their resolution

The next step in my analysis of ethics guides was to look at them in more detail, particularly the kind of ethical issues that they identify. The purpose was to check

for any differences between 'general' ethical guidance provided by universities, professional associations, governments, private organisations; and online social research specific ethics codes. Again, the rationale for this approach is that if there is a considerable overlap of ethical issues then online social research does not represent an entirely new research environment. In this case one may even argue that we do not even need 'new' (= extended) ethics codes but can just apply the basic principles of 'general' ethical guidance as they will suffice to manage online research risk.

When analysing the guidance one can quite easily identify a number of key ethical issues that appear throughout 'general' ethical guidance. Depending on the target audience and the purpose of the ethics code these key issues are considered more or less important. Nonetheless, those identified here are the ones that are present and considered of particular importance throughout. They include: informed consent, confidentiality, anonymity, privacy, participants' rights, vulnerable groups, research relationships, coercion, and reporting of findings. When studying online social research specific guidance one can see that the above key issues are also present in them. This in itself is further evidence that the research environment –namely, the Internet and cyberspace – is not as radically different as some academic and popular conceptualisations would like us to believe. They are not that different from offline social environments because the key ethical issues identified offline and online are one and the same. Here I am not necessarily referring to practical 'sameness', but rather to 'sameness' in principle (see section 2.2.2).

However, there are also potential claims of difference introduced by online ethics guides. Online social research guidance present several issues that are considered of critical ethical consequence: pseudonyms, the blurred distinction between the public and private sphere, restrictions on what can be researched set by the subject group, and the question of whether the participant is a human subject or an author. I will address each of these issues in turn to reflect on the question of how far they are mirrored in current offline social research practice.

The issue of the pseudonym arises due to the common practice of Internet users creating pseudonyms for themselves while online. These pseudonyms are more often than not freely chosen identifiers that are not the user's real name. This is thought problematic and thus an ethical issue in that it reduces the researcher's ability to assess how far the person they are communicating with is believable and even potentially from a vulnerable group (Stern, 2004; Sassenberg and Kreutz, 2002). This issue is intensified by the idea presented to us in some academic as well as popular conceptualisations of the Internet and cyberspace that people while online mostly experiment with identity play and thus are less credible. While chapters three and four clearly show that the regulatory framework and resulting interactions are far more restrictive than that, this popular misconception is nonetheless very influential in the creation of this ethical issue. However, as I disagree with this position, the use of pseudonyms in terms of credibility is of less consequence to me. Furthermore, and more to the point of this chapter, the underlying issue is not new. The ethical or methodological issue that is really addressed here is verifiability. Something that the online research specific guides

forget to mention is that really, the issue they raise is very much present in 'traditional' mail questionnaires too. Using this method one cannot be certain who fills in the questionnaire, just as much as we cannot necessarily always be certain of the 'real' identity of our online subjects. However, there are much more immediate means to check online identities than offline ones. Here I refer back to some of the ISP activities outlined in the previous chapter such as data profiling or even more immediate by using a standard search engine. The key point to appreciate is that while pseudonyms are a special 'reality' in the 'new' research environment that is cyberspace the key ethical and methodological issues that they bring about are already considered, in principle, in 'general' ethics codes.

Another underlying issue to do with pseudonyms is that of traceability. This is the possibility to potentially track down respondents via use of their pseudonyms due to technological opportunities offered by the Internet. Traceability itself is not new; however, the technological tools provided to us by the Internet make it a simple point and click exercise. Therefore, I argue, that the real ethical issue is not traceability but rather anonymity, confidentiality, privacy, risk vs. benefits, and causing no harm. Traceability is not the ethical but the practical issue, enhanced through technology that demands a more in depth reflection on the ethical issues which arise due to this technological possibility. Hence, the issue of pseudonyms in conjunction with traceability is not an ethical issue per se rather it is a practical issue that leads to the question of how we can meet the ethical demands of confidentiality, anonymity, privacy and causing no harm in an environment that makes tracking down participants by just about anyone so easy.

A further ethical issue that is raised is that of the blurred distinction between the public and private sphere. Again this ethical issue arises for two reasons: First, the definition of cyberspace as a public sphere; second, researchers being rejected by potential subjects. The first point has been illuminated and then rejected in chapters three and four. Still the majority of online research specific ethics guidance is built upon the idea that cyberspace is a public sphere. What surprises me is that those in the field leading on creating online social research ethics codes still rely on this outdated and 'illegal' conceptualisation of cyberspace. I argue that the main reason for a recognition that there is a blurring of the public and private sphere stems from negative research experience. This negative experience manifests itself in that researchers report that their subjects considered their communications private and thus 'chased' the researcher away. There is such a strong feeling about not wanting to be research subjects now that users make explicit in their terms of use agreements that no online research is to be carried out or if then only with explicit permission (Williams and Robson, 2004).

Certainly this is evidence of poor ethical practice in the past and the negative outcomes for users and researchers strongly suggest a need for new ethical guidance. However, I believe that it is not so much new ethical guidance that we need but an updated understanding of cyberspace as a space that consists of places that are to a varying degree public or private. There is some evidence (University of New Hampshire, 2005; NENT, 2003) that online social research ethics codes are beginning to move in this direction. Currently, they recognise that cyberspace consists of several venues. However, the fact that these venues

have internally and externally socially (and legally) created norms, values, understandings of themselves, as well as differing levels of privacy still needs to be made explicit and added to these ethics codes. The important step that needs to follow is that online social researchers should apply this nuanced understanding more readily.

The final key ethical issue that is presented to us in online research but not in 'general' ethical guidance is the question of whether users are human subjects or authors. This is a rather crucial question because if we decide that they are authors, social researchers can ignore the majority of ethical issues that would be of concern if they were human subjects. Again, this is not so much an ethical issue as one that is rooted in the conceptualisation of cyberspace and the nature of the communications occurring within or via it and has to be resolved before one even begins to design ethical guidance. I suggest that generally consensus is that online respondents are human subjects rather than authors (Roberts et al., 2004). However, what makes it more difficult is legislation and regulation based on copyright and intellectual property. The internet allows access to materials that have been created with an economic intent by individuals who see themselves as authors and thus want their online communication to be recognised as such. Again, the social researcher has to engage with this matter to ensure that his or her respondents' communications are treated appropriately.

Some of the 'general' ethics guides but mostly the specific online research guides of my sample provide further explanations of difference between online and offline

research ethics. RESPECT (2004) is one of the general guides that states that online ethics differ from offline ethics. This it is argued is due to the risks inherent in electronic data processing and transfer. Confusingly, it is then declared that there is no need for new ethics for online social research only particular caution as online research poses greater risks. I believe that what this code is trying to say is that this risk is not due to a previously unknown ethical dilemma, rather the risk of the known dilemma is increased by the technological realities of the Internet. This concern is mirrored in current online research specific guidance. There are overall three areas of difference suggested in them: 1) environmental difference; 2) difference in magnitude; 3) difference in security and risk.

The code produced by the AoIR (2002) tells us that online research takes place in a range of new venues and argues that new ethical issues arise that are not directly addressed in extant statements and guidelines. It further makes us aware of the global scope of online research, meaning that our ethical considerations have to take account of different national and cultural frameworks. This view is supported by the University of Sheffield (2003) placing emphasis on the 'newness' of contexts of human interaction that make up the Internet and cyberspace. The American Association for the Advancement of Science (AAAS) agrees with the prior assertions. However, it points out that while the environment is different and adds to concerns, the issues themselves do not differ. Based on my argument thus far, I find myself in agreement with the AAAS. The difference in environment means that we may have to spend more time on certain ethical

issues than we would have to in the offline context. However, those ethical issues can and have been of concern to previous – more traditional – research too.

The second key theme is the difference in magnitude. "The issues raised by Internet research are ethical problems precisely because they evoke more than one ethically defensible response to a specific dilemma" (AoIR, 2002). The AAAS (1999) gives us a more detailed list of difference in magnitude including "may increase subject's risk of exposure", "difficulty to gauge risk to subject", "deception offline ok at times but real uncertainty whether it is an ok approach online", "anonymity of online interactions is fundamentally different from that of traditional practices". When considering the size of the Internet, the number of potential users, the variety of cultural and social contexts, and the number of technological possibilities that do not exist so readily offline; then one cannot disagree with the sentiment that one of the key differences between offline and online research is magnitude. However, again, the purpose is not to agree on difference, but to assess whether this difference - here magnitude - results in the need for new ethics guidance. Magnitude itself is not an ethical issue. Thus, based on the evidence and the above discussion, there is no necessity for new ethical guidance, rather the need to recognise the issue of magnitude and reflect on how it impacts on our research practice to remain true to ethical practice.

The final area of difference lies in the nature of security and risk. The University of New Hampshire (2005) points out that the digital nature of cyberspace and Internet security issues demand quite a different focus. According to its guidance,

offline data security is also a concern but normally is not more than a small practical issue. This is more evidence that online ethics guidance sometimes confuses an increase in a need to consider a particular ethical issue due to the technological reality of the Internet and cyberspace with this constituting a new ethical issue (see section 2.2.2). The concerns of data transfer and security are tied up with the matter of traceability discussed above. They are tied up in so far as while being correctly identified as a marker of a possible difference between some areas of online and offline research; they are not new ethical issues themselves nor do they change 'traditional' ethical issues (see section 2.3). What they do is to require us to spend more time considering those ethical issues on which they impact to ensure that our research practice in this different and new social environment remains ethical. Therefore, one may not need the creation of new ethics codes as such, but rather an updating and extending existing guidance to reflect the practical dimensions of social research that includes online enquiry.

The next element of ethics codes to think about are the resolutions to the above ethical issue that they offer. This is the final 'test' to detect any difference between the offline and online research environment that is based on the comparison of offline and online ethical guidance. When analysing the suggested responses to the ethical issues of social research one may identify several key resolutions. The first key resolution is that of obtaining informed consent. The majority of guidance in my sample makes it a priority to obtain informed consent. There are differences around when to obtain this consent and how and

disagreement on the merit of covert research. But overall obtaining informed consent is a key activity to ensure ethical research practice.

The matter of informed consent is also a key issue in online social research ethics codes. However, the disagreement lies in when it is necessary to obtain it as there is the conceptual dilemma of whether cyberspace is a public or private space. In response some guides suggest that researchers should consult their potential subjects to establish whether they consider their communications public or private. If they consider it public then, it is argued, there is no need to obtain informed consent. This is a significant departure from offline research where this approach is not used. However, again, the underlying ethical issue is the same and it is only the environment that means that we may take a different approach to ensure upholding this ethical value. Thus, I suggest, that we need to update current general guidance on social research by providing either detailed guidance on how to proceed in such environments or by raising researchers' awareness of the environmental impact and opportunities when considering a particular ethical issue. The other key ways in which to address the key ethical issues outlined above are identical in online and offline research guidance. Some online specific ethics codes go even so far as to state that it is assumed that researchers know how to resolve them by sticking to previous ethical guidance (University of New Hampshire, 2005).

The only discernible difference is the practical ways in which these resolutions are to be realised. Taking this into account then it would make sense to produce a

specific online research ethics code. This code would not deal with different ethical issues or even different ways of addressing them, but be a practical instruction on how to do it. The only reason for it being produced would be because the level of detail would be too complex to be included in a general ethics guide. However, the discipline managed to write ethical guidance that incorporated many differing research environments into a general ethics code before. Therefore, we may have to do two things: Firstly, produce a general ethics guide that takes online social research into account; and secondly, produce a detailed practical guide on how to translate that 'theoretical' ethical guidance into practice.

6.2.4 Claims of difference and newness unmasked

By comparing and contrasting online and offline specific social research ethics guides I was able to identify several key points. They are:

- The claims being made within ethics codes suggest that we may need an extension of or a shift in focus of ethical guidance to incorporate online social research.
- There is sufficient ontological and epistemological overlap between online and offline specific ethics guides to allow an extending and up-dating of 'general' ethical guidance to include the online social research environment.
- The key ethical issues identified by general and cyberspace specific guidance are the same.
- Claims of difference between online and offline research ethics do not stand up to scrutiny.

- There is a difference of magnitude/ amplification and other technological realities that distinguish online and offline social research. However, they are not ethical issues in themselves.
- These differences of research environments have to be taken into account when thinking about ethical issues.
- Online and offline guidance suggest the same resolutions to these key ethical issues.
- The key reason for difference between traditional and online specific guidance lies in the uncertainty over the conceptualisation of cyberspace. The more one defines it as unlike the offline environment the higher the need for adjusting general ethical guidance in order to manage risk in online social research.

Considering the above themes, I am at this point able to argue that the initial sense of difference of research environment, difference in ethical issues and the resulting merit of a call for new ethical guidance was inappropriate. The evidence provided in this chapter shows that there are clearly marked differences between traditionally offline and more recent online research environments that pose questions for our ethical guidance. What they do not do, however, is to pose new ethical issues. The questions they pose impact on ethical guidance in a way that suggests current general ethics codes need to be extended and up-dated in order to address a) the situations in which these ethical issues occur/appear in cyberspace; and b) the practical ways in which those ethical issues are to be resolved in the online context. Therefore, an extension of ethical guides should

not be motivated by creating new categories but by reflecting how to work in an ethical manner within the particular environments that social researchers are currently active in. This does not necessarily discredit the raison d'être of current stand-alone online social research specific ethics codes. These codes are necessary in order to reflect upon the impact of the perceived difference of the research environment on ethical research practice and are needed to make up for the lack of this undertaking in current 'general' social research ethics codes.

Thus, based on the comparative analysis of general and online specific research ethics codes, the answer to the question of "can current ethical guidance of social research manage the risk in online social research" is - not quite. It appears that we do need 'new' ethical guidance. However, I have to clarify this by defining 'new'. The 'new' means that we do not need to develop new ethical categories, but we have to amend and extend currently existing mainstream guidance to reflect our recognition of a difference in magnitude, between the online and offline social research environments, that impacts on certain ethical considerations.

6.3 Investigating legislative issues for cyber ethics

Having established the merit of new ethical codes for social research from a purely ethical point of view, I will now assess how far current ethical guidance can resolve the issues that arise due to Internet legislation and regulation – as outlined in chapter five. I am less interested in comparing offline with online specific guidance as it is more pertinent to establish whether current ethics codes provide sound resolutions to the issues at hand. My argument is that if current

guidance can resolve those issues satisfactorily then we can proceed as outlined under section 6.2.4. If this is not the case then we have to add further amendments to ethics codes that go much deeper than envisaged thus far. To carry out this assessment I begin by outlining the legal guidance that is provided by ethics codes. This serves as a backdrop to the following discussion. Then I analyse the effectiveness of current ethical guidance in dealing with the ways in which key ethical issues arise due to legislation, regulation and online activities. The key ethical issues identified in chapter 6 and addressed here are: (1) informed consent; (2) confidentiality, anonymity and privacy; and (3) safeguarding researcher and subject.

6.3.1 Legal guidance in ethics codes

Most ethics codes contain a reference to legislation that is deemed of relevance to the particular research practice that is targeted. The list of Acts that are referred to in my sample of ethics codes include: The EU Data Protection Directive 1995; the UK Data Protection Act 1998 and 2001; the UK Computer Misuse Act 1990 ; the Equal Opportunities Act; the Race Discrimination Act ; the Obscene Publications Act ; the Protection of Children Act 1999; the UK Freedom of Information Act 2000; the Copyright Act 1988; the US Privacy Act; the Human Rights Act 1998; the Human Tissue Act 2004; the Medicine for Human use Regulations 2004; and the Health and Safety at Work Act 1974. While all these Acts appear in the sample, in reality ethics codes only draw on one or, at most, two of the above at a time. The only exception to this is the RESPECT (2004) code in which law is a key part of the guide. The majority of the guidance

predominantly draws on Data Protection Acts. However, the extent to which Acts are actually deconstructed and their relevance to social research practice explained, and the issues raised - varies greatly.

When ethics guides do discuss legislation they point out several things including: that the privacy of data is not privileged under law; that we need permission to collect data; that we have to ensure confidentiality; that we have to store the data appropriately; that we need to comply with copyright legislation; and that researchers should acquaint themselves with the relevant national and international legislation. Why this is the case, how and when one is to respond to these matters is not discussed.

When comparing online with offline specific guidance surprisingly online research ethics codes show very little engagement with legal matters. They do state that researchers should respect the laws of the countries under whose jurisdiction the research and the subjects find themselves. They point out implications for consent due to Data Protection Acts and raise the issue of 'legal' data interception. However, they neither give details of when or how these issues arise and why they matter, nor provide any actual guidance on how to resolve those legal/ethical issues. This is surprising considering that their only real claim to difference and thus the need for new ethics is founded in the socio-legal conceptualisation and construction of cyberspace. Thus not engaging with legal considerations properly represents a considerable shortfall.

It is appropriate to state that my analysis has shown that guides are treating laws only fleetingly and in a rather superficial manner. Often ethics guides only state that such and such act has to be kept in mind or that a particular issue may be problematic usually without providing clear evidence, explanation or resolution. This is surprising as at least some of the guides (SRA, RESPECT, ASA, BSA) do argue that engaging with laws has been and is becoming more important. One example of this is the following statement "…recent legislative changes and concerns about litigation have increased funder's interests in and concern about good ethical practice in social research" (SRA, 2003). Another example of this is the advice by the ASA (1999) that even if there is no law on confidentiality one is to still act as if there was. Recognising that there is an acknowledgment of the importance of, yet at the same time, an apparent lack of serious engagement with legislation in current ethics guides one has to question how far these ethics guides can then be of use in navigating the key legal-ethical issues of online social research as identified in chapters four and five.

6.3.2 Challenges to informed consent

In order to analyse the question of whether current ethical guidance is effective in addressing online social research issues that arise due to legislation, regulation and online activities in detail I begin by analysing the issue of informed consent. I do this by focusing on three issues: 1) informed consent and covert research; 2) informed consent and 'double' data collection; 3) informed consent and parents. For social researchers to obtain informed consent they have to follow certain procedures and provide their potential respondents with adequate information

about the research project. This key principle of social research ethics "implies a responsibility on the sociologist to explain as fully as possible, and in terms meaningful to participants, what research is about, who is undertaking it and financing it, why it is being undertaken, and how it is to be disseminated" (British Sociological Association, 1991). When reviewing ethics literature one can discern a detailed breakdown of the areas on which a subject ought to be informed on in order to be able to give their informed consent. They include information on:

The purpose of the study.

Who the researcher is.

Who collects the data.

What data will be collected.

When and for how long data is collected.

How the data is collected.

Who has access to the data.

When the data is accessed.

How the data will be used.

How the data will be published.

Whether there are any risks to the subject through participation.

This list complies with current Data Protection legislation, yet there are still some social researchers who believe that retrospective consent or covert research without consent are credible forms of research (Homan and Bulmer, 1982; Herrera, 1999). The Internet and cyberspace to these researchers is an almost

endless source of data at their fingertips and all they need to do is 'cut and paste'. This attitude betrays several of their positions. Firstly, they believe that the Internet and cyberspace are a public sphere of interaction. Secondly, they often put into question whether what they see online stems from human subjects or authors.

Current ethical guidance does not necessarily endorse covert research; however, it does not reject it either. Nonetheless, according to current Data Protection Acts (DPA) covert research is illegal. Even though the RESPECT (2004) guide does translate what the DPA means for social researchers, it does not include the fact that data subjects have to be informed and consent to their data being collected. Furthermore, some Internet Service Providers (e.g. YAHOO!) have put policies into place that mean that users of their services are not permitted to gather data of/on other users. Last but not least, many Internet user communities have stated in their terms of use agreements that no data shall be collected on them by researchers without prior explicit consent. These three layers from law, regulation to online user activity mean that social researchers are required to request informed consent thus ruling out the use of covert research. How do ethics guides suggest we deal with this reality? Covert research is a controversial part of the methodological repertoire of social scientists. Does the legal framework of the online sphere mean that we cannot use it any longer or is there an ethical way around this impasse?

The majority of the ethics guides that I studied provide researchers with a rationale for carrying out covert research. I present here three examples to illustrate this. The first example is that of the Social Research Association SRA (2003) which tries very much in its guidance to restrict the impact the law has on research practice by what I consider yielding as little ground to the Data Protection Act (DPA) 1998 and the Human Rights Act 1998 as possible. It argues that consent is not a precondition of all social inquiry and that researchers have a rationale for how informed their subjects can be considered to be. The second example is that of the International Sociological Association ISA (2001) which argues that informed consent is necessary unless there is no other way to gather the relevant information or if access to the information is obstructed by those in power.

The third example is the American Sociological Association's ASA (1999) guide stating that researchers may seek a waiver for consent if their research presents only minimal risk to the subject or if it were not practical were informed consent required. The American Psychological Association APA (2002) provides a much more in depth explanation on the appropriateness of not obtaining informed consent. It can be dispensed with: "1) where research would not be reasonably be assumed to create distress or harm and involves a) the study of normal educational practices, curricula, classroom management methods conducted in educational settings b) only anonymous questionnaires, naturalistic observations, or archival research for which disclosure of responses would not place participants at risk of criminal or civil liability or damage their financial standing, employability,

or reputation, and confidentiality is protected; or c) the study of factors related to job or organization effectiveness conducted in organizational settings for which there is no risk to participants' employability, and confidentiality is protected or 2) where otherwise permitted by law or federal or institutional regulations" (The American Psychological Association, 2002).

None of the above ethical guidance either addresses the specific realities of the Internet and cyberspace or offers a justification to ignore or circumvent the legal, regulatory or online community rules basis which requires us to obtain informed consent. Therefore, there is a clear tension between ethics and the law. The tension arises because ethically, social researchers may justify their use of covert research in offline and even some online settings. However, the legal framework in place means that those ethical justifications are ineffective. We are not legally able to carry out covert research in cyberspace. Furthermore, we are not ethically able to carry out covert research in cyberspace because our own ethical guidance tells us, and this is also based in Data Protection law, that we have to give potential respondents the right to not participate in our research.

Nottingham University's Research Code of Conduct and Statement of Research Ethics (2000) is one of the very few examples that does not make a provision for covert research and instead relies on the Data Protection Act of 1998 to state that researchers need permission to collect data. This university's code is one example that would at least enable a social researcher to begin with online social research. However, as it misses out ISP and user regulations, it falls short of the kind of

guidance that is ultimately required. It falls short because it would not prevent a researcher from breaking ISP terms of service and privacy regulations and upsetting online communities because it does not make him or her aware of the need to engage with those during the design and planning stage of his research project.

The second issue is that of informed consent and 'double data collection'. In chapter five I have already discussed in detail the fact that current DPAs and resulting ISP regulations mean that we are not the only ones gathering data on our research participants. As a matter of fact ISPs collect data even prior to our own data collection they collect data that mirrors our own; they collect data that lie outside of our research activities; they use third parties to collect bits of data on our respondent; they actively purchase data held on our research participants by third parties; they use techniques such as data profiling to bring all this data together; they are vague in how the above works and when/why it occurs; they are vague in defining who has access to the data, and how it is to be used; and they hold on to the data even after the cessation of the service contract . Again these activities are not illegal and our research respondents are not (usually) the individual target of ISP activities, but this is what happens to our data when we interact online. Interestingly, we all have to and do agree to these activities every time we sign up to or make use of ISP services.

In chapter five I argued that this results in 'double' data collection. By this I refer to the fact that two types of data collection occur in parallel – that of the

researcher and that of the Internet Service Providers. Neither has got anything to do with the other. As conscientious social researchers considering the kind of information that we need to provide in order that our potential respondents can give us their informed consent we have to ask ourselves several questions:

- Do we have to inform respondents on how ISPs interact with their data?
- Can we obtain informed consent if we cannot fully inform our subjects on how, when, why and which data is collected and what happens to it?
- Can we accept informed consent given by potential respondents if we are not certain that they have not necessarily got all the information that they need to make such a decision?

The law as well as ethical guidance are a little bit unclear on their answer to the first question. This is because both are very focused on targeting their provisions on the specific data collector. This means that when they talk about obtaining informed consent they only demand that collectors inform subjects about the data that they are planning to collect. There is no clear reference to the collection of data by third parties in terms of gaining informed consent. No guidance is offered on the fact that the social researcher involving subjects in online research automatically results in 'double' data collection as ISPs will start collecting data as soon as the respondent signs up to the ISP service in order to interact with the researcher or his/ her research materials (website, email or web based questionnaires etc.). Furthermore, the respondent agrees to the terms of service policy and privacy policy statement of the ISP when signing up to the service and then agrees to participate in our research thus consenting to both forms of data

collection. At this point this may suggest that the researcher can just ignore the fact of 'double' data collection and only inform the participant on their research specific procedures.

However, this is when other guidance on the need to protect confidentiality, anonymity, privacy and preventing harm need to be considered. Taking these criteria into account means that social researchers do have to inform the research subject on ISPs' and other groups' data collection activities. This is because these activities may well have adverse effects on the research participant that arise due to their interactions with us and their use of ISP services. It appears that ethical guidance is sufficient to resolve this ethical issue. However, the problem is that I have become aware of this first question only after engaging with legislation and ISP regulations – something that the majority of online and offline researchers have not engaged with thus far. This means that current ethical guidance, while ultimately enabling us to resolve this first question, needs to raise awareness that this first question has to be asked in the first place. This is necessary to ensure that social researchers provide their potential participants with the relevant information for them to make an informed decision to participate and thus enable them to give their informed consent.

The second and third questions arise due to the fact that ISPs and third parties are very vague in their explanation of how, when, why, for how long they collect data and what they do to it. There are currently moves undertaken by governments and ISPs to rectify this vagueness, but considering the immense size

of these companies and their outsourcing practices to third parties it will, arguably, always be very difficult to gain a full understanding of what is going on and therefore fully inform prospective subjects. The law, however, requires us to fully inform our subjects and so does ethical guidance (now that we have dismissed covert research). At this point we would have to consider that certain research projects would not be tenable as we may not be able to fully inform our respondents. However, this position is too extreme and rather patronising. It assumes that the researcher is all-knowing in terms of what is best for the participant and that the respondent is in need of protection. This is consistent with earlier forms of ethics and is to some extent mirrored in certain elements of current research governance. Nonetheless, this ethical approach would a) potentially disrespect the intelligence and self-determination of subjects; and b) potentially handicap possible research activities considerably.

Therefore, drawing on a more liberal framework, I would suggest it is sufficient to require researchers to inform subjects on which ISP policy documents to read prior to consenting. This would evidence our commitment to good ethical practice and to respecting our potential research respondents. This approach is not universally applicable though, as it would have to depend on the respondent's ability to understand and judge the risks and the subject to be studied. Again, the basic ethical principles have prevailed and enabled us to resolve this issue successfully. However, this was only possible after incorporating and applying an understanding of how legislation and regulation impact on online social research practice. Therefore, current ethical guidance on its own does not suffice but has

to be supplemented by adding the need to enable the potential subject to engage with ISP data collection policies in order to receive informed consent. This may well mean that our usual covering letters and consent forms have to be restructured, quite possibly to resemble much more the business style policy documents of Internet Service Providers (ISPs).

The final issue to be examined regarding consent is that of informed consent and parental consent. In current research practice the majority of ethics codes still rely on the concept of parental consent or guardian consent when addressing research with children and underage respondents. This is very much based on what Lee (2001, 2004) describes as the idea of children as human becomings. More recently, there is a move towards 'listening' to the children themselves and allowing them to have more say in whether they want to participate in research and hearing their uncensored voices. As discussed in detail in chapter 5 the default position in law is that for any kind of data to be collected from children the parents have to give their informed consent first. They have to be provided with information on what data is to be collected, when, for what reason, the use of the data, and the disclosure practices. The difficulty in the online context is that the only obvious way to gain access to the parent and to ask for their informed consent is by asking children for their parents' contact details. This, however, may already be considered an illegal activity as it would be understood as data collection without prior parental consent.

Within my sample of ethics codes the UK based codes make it perfectly clear that respondents under the age of 16 need parental consent. As to how this is to be achieved is left to the researcher. However, many guides provide researchers with ways around this requirement. Barnardo's (2007) guide gives several reasons for when parental consent is not needed. They include: research involves minimal risk; consent is impossible or would not protect the young person/child; consent would be resisted by young people due to the desire to protect their right to confidentiality and privacy; risks of participation are regarded to be low. Again, this kind of ethical guidance shows an entire lack of engagement with the legal framework within which research is undertaken. Following the above ethical advice may mean that we are ethical but also certainly open researchers to the risk of potential legal prosecution. Here is another example of the tension between ethics and law that arises out of the legal framework and conceptualisation of cyberspace. Even if researchers were to attempt to gain parental consent, current ethical guidance remains silent on how to achieve this in online social research. In particular, the issue of not being allowed to contact children to ask for their parental personally identifiable data (PID) is not addressed.

The law has, however, provided a solution in this case. It states that if the data collected from children is only used to gain parental consent and is, when no consent is given, destroyed then data collectors may ask children for PID of their parents prior to parental consent. The remaining issue is that this particular legislation is applicable to US citizens only. The question for social researchers is

how to negotiate this dilemma in other jurisdictional contexts in a multi-jurisdictional cyberspace environment. Again, current ethical guidance that I analysed does not reflect this issue. It does not tell us that parental consent does not entail the same meaning or procedure everywhere. It does also not tell us how to resolve the issue of parental consent in the UK context where there is no legislation like the aforementioned US Act.

There is one exception when there is no need for parent consent, at least in the US. The US Children's Online Privacy Protection Act (1998) states that it is unnecessary if the Commission determines that it is appropriate to forgo parental consent, taking into consideration the benefits to the child of access to information and services and risks to the security and privacy of the child. This is problematic. Does it mean that if our research was on sexual health, or emotional issues, or other personal matters we need not worry about parental consent? Here it appears as if legislation is opening up a back door for social researchers. Can we, in case of such research, ignore the ethical guidance and requirement of parental consent? Again, this is all rather vague. What is the merit of the Commission? Where does its ruling apply? Can parents use other laws to counter researcher activities? These are all questions that are currently not addressed in ethics guides. Furthermore, according to current Data Protection legislation 'personal' opinions of children do not count as personally identifiable data. Does this mean that we do not need parental consent if we just collect personal opinions? Do we have to grant parents access to this data? Guidance such as that of Barnardo's (2007) would answer yes to this in most cases. However, that guidance is not

applicable as it was conceived in a context in which these questions were not posed. Therefore, we do need to revisit ethical guidance and develop our answers to these questions with the current legal framework in mind.

As already pointed out in chapter five, one thing the analysis of current legislation makes abundantly clear is that past approaches that allowed for consent by gatekeepers do not hold merit any longer. They may still be appropriate in an offline setting. However, online, this is not the case. None of the legislation that addresses online data collection from children mentions a provision for gate keepers as a possible source of consent. Also, from an ethical point of view we would have to ask ourselves whether we can justify accepting informed consent on behalf of children from operators who may be underage themselves, do not know the potential respondents, or may not be accepted by potential respondents. These questions, however, are not currently incorporated into social research ethics codes.

Overall, this section on informed consent has shown that while basic ethical principles can help us to navigate and resolve the issues that legislation and regulation cause in online social research environments, current ethical guidance does not. Current ethics codes do not suffice because they do not even address these issues in the first place, and therefore if one was to follow their guidance one may not be able to obtain properly informed consent. Furthermore, our misguided actions may quite possibly break several laws, regulations and upset online communities.

6.3.3 Challenges to confidentiality, anonymity and privacy

The second key issue identified in chapter four is that of confidentiality, anonymity and privacy. These ethical issues are presented as one issue because they are inter-linked.

As outlined in detail in chapter five, ISPs actively collect personally identifiable data (PID) of their users. This poses problems to social research ethics in that it runs counter to our desire and ability to protect the confidentiality, anonymity and privacy of our respondents. Added to this are the surveillance activities of other groups and organisations such as the police and charities which further undermine the privacy, anonymity and confidentiality of our research communications, respondents and us. Two questions arise in this situation: 1) Do ethics guides resolve this issue? and 2) if not, do we have to surrender our claim to being able to protect the privacy and anonymity of respondents and offer of confidentiality? Reviewing the ethical guidance in my sample I am able to argue that ethical guidance does state that we have to offer confidentiality, anonymity and privacy to our respondents and take appropriate actions to realise these aims. However, they do not tell researchers about the problematic context of the Internet and cyberspace and consequently they do not provide an answer as to how to achieve these aims in this particular context. In this case ethics codes fail to recognise that it is not possible to offer complete confidentiality, anonymity or privacy in online social research. In this they provide further evidence for the need of new ethical guidance.

One main issue raised in online social research methodology debates is that it is difficult to verify the identity of research participants. As argued earlier, this is not only the case in online research, but has become one of the main sources of criticism of it. The fact that ISPs and others do collect PID on our subjects that go beyond our own research merit and abilities, also offers interesting opportunities. For one, access to ISP PID on our respondents would certainly enable users to verify the identity of our subjects. This while not currently practiced by ISPs, may be an interesting future methodological development. However, our ethics guides have not addressed this possibility as of yet and are thus not able to provide appropriate guidance on the matter.

Returning to the issue of not being able to fulfil our ethical aims of providing confidentiality, anonymity and privacy due to ISP and other online activity; a possible response to this issue may be to actively hide the identity of our research participants from them. There are several possible ways of doing this which would be illegal and break Terms of Service agreements of Internet Service Providers (ISPs). Following this course of action is, however, the only possible way that I can currently see in order to remain true to ethical guidance. This is another example of the tension between ethics and the law that arises because ethics codes have not taken legal developments into account. Therefore, one has to revisit ethical guidance to establish ways in which we may resolve this issue and actively engage with legislation in order to create space within it for online social research.

Another question to consider arises out of the fact that ISPs collect different data to that of researchers and do store this data differently. The ethical question to address is "Are we responsible for the protection of the confidentiality, anonymity and privacy of data that we did not even collect and that exists after our actual research has already finished?". In the case of our own data on our subjects ethics codes answer with "Yes". However, this particular situation has not presented itself before and thus 'general' ethics guidance is ill-equipped. More concerning is the fact that even online specific ethics guidance has not addressed this question either. Therefore, this is further evidence that more ethical consideration and subsequent guidance is needed.

One final issue that has emerged in chapter five is the question of when we can break our commitment to confidentiality, anonymity and privacy. The example given was that of research where one of the research subjects committed suicide and the researcher had chosen not to report the subject's state of mind prior to her taking her own life. In chapter five I stated that it was the legal obligation of the researcher to do so. When approaching the issue from an ethical point of view, my sample's ethics codes fail to provide a clear answer about when to forego these ethical aims. The only thing they do is to tell the researcher to ensure that they prevent any harm caused by the research. However, this is not what happened in this example. The research itself had nothing to do with the tragedy. It is understandable why ethical guidance is so silent on this issue. The aim of naturalistic research represents a strong current in ethics guides and explicitly requires we try to avoid impacting on the research field. However, we

do have to question at what price. In this situation we do not even need to develop new ethical guidance. All that is necessary is an implementation of current legislation that requires the reporting of data that shows a risk to life, danger to society or a crime being committed. This in itself represents tensions between ethics and the law; nonetheless, ethics guides have to be updated.

This sub-section has shown how the issue of confidentiality, anonymity and privacy are addressed in ethics guidance. However, the guidance is inadequate as it fails to incorporate legal developments that have a considerable impact on the ways in which we think about these issues and how we are to resolve them.

6.3.4 Challenges to safeguarding researcher and subject

The final issue to be considered is that of safeguarding the interests, rights and well-being of researchers and their research participants. In this section I draw on the issues that I first identified in chapter five to analyse in how far online researchers are able to safeguard their subjects' and their own interests, rights and well-being by following current ethical guidance.

One of the issues mentioned several times already is the fact that ISPs collect and have access to the personally identifiable data of the researcher as well as her or his subject's. This requires us to ask whether this affects our ethical practice. One way in which this affects our practice is that neither researcher nor subject are in control over the possible outcomes of this. They may receive unwanted advertisement, or may be contacted by third parties for other purposes than those

associated with the research project. When consulting ethics guides we are told to safeguard our respondents from unwanted intrusion, harassment or any kind of harm. This is also what the Data Protection legislation requires of us. However, there is no obvious way in which we can protect our respondents in this situation. Current ethics guides do not appear to address this reality of online social research.

This particular issue is heightened as soon as we think about the surveillance practices of law enforcement agencies, the police, ISPs and other private organisations. They all carry out surveillance, gathering data on online communications and activities. Occasionally they will present ISPs with court orders (in the case of the UK) which require them to present PID about particular users. This happens without the knowledge of users. Furthermore, ISPs themselves carry out surveillance and will disclose personally identifiable data if the user has broken their Terms of Service Policy or if they have broken laws or are involved in criminal activities.

The problem with these ISP actions is that ISPs are purposefully vague in their public representations and their use of defining terms within the trigger mechanisms. This vagueness was already discussed in detail in chapter five, but the basic consequence of it potentially is the false accusation of researchers or their participants, the wrongful interruption of research activities and communications, and the potential of unnecessary and ultimately unjustified legal action. This may well mean that no controversial topic ought to be studied via or

on the Internet. Furthermore there remains a risk, however distant, of encountering foreign surveillance by suppressive regimes (Karatzogianni, 2010). Even if we were to communicate with immigrants about their country of origin and their reasons for leaving, their home country may intercept this communication and take action either against the immigrant directly or against his or her family members who remain in the home country. That this is not such a farfetched scenario is evidenced by the recent trial of and verdict against a Chinese scholar who was found guilty of subversive use of the Internet. Does this mean we should not research political issues either?

Again, how do the ethics guides in my sample resolve this issue? They do not. Even though the underlying issues are similar to those faced by criminologists and have been inventively negotiated by them, the fact that potentially every communication may be used out of context and against researchers and or their participants requires renewed engagement with the matter. In offline social research much can be carried out 'under the radar'; in cyberspace this is increasingly impossible. In the end we have to ask ourselves what it means to social research practice to possibly produce communication data that may become part of a prosecution case, even in another country.

Similarly problematic is the study of child abuse. This topic is of particular interest to certain social researchers as it is an offline phenomenon that has moved online and goes through regular cycles of moral panic. As outlined in the previous chapter it is illegal to carry out any kind of research on Internet child abuse and

even looking for the offending material will result in one's name appearing on the sex offenders register. Furthermore, police use so-called 'honey-traps' where they pose as children and actively engage in communications with adults (see sections 1.1.2; 3.2.2.2). They do this in order to catch adults who are seeking to communicate with children in inappropriate ways. These activities pose a real risk to social researchers. What if we were to study teenage pregnancy via the Internet, using online interviews and chatrooms in order to gather data from under age respondents? What would happen if we were to talk to an undercover police officer? Would our communications be considered inappropriate, dangerous, or illegal? Does our ethical guidance protect us from falling into these honey traps?

This is not raised in my sample of ethics codes. They do not warn the researcher of the potential danger of becoming the target of an investigation or being falsely accused. The only way to avoid this problem, while still enabling us to study the issue, is to be completely open about one's own identity and to seek informed consent. Covert research - even though illegal anyway - could have disastrous consequences. Again, applying the ethical principles and thinking through them allows us to resolve the issue. However, without applying my knowledge of police activities and techniques to the ethical considerations, I would not have been able to do so. Yet again, ethical guidance is not appropriate for current times as it lacks the knowledge of and incorporation of online policing activities into its guidance.

This sub-section has demonstrated that due to surveillance activities and current data collection policies and laws, researchers have to reflect ethically on how to ensure that they and their subjects are safe. Analysing the usefulness of ethical guidance shows, however, that it is not able to protect the researcher and his respondents because the guidance is not informed by current police, public and private organisations' online activities and practices. Thus, there is a need to reconsider how to safeguard our and our research subjects' interests by up-dating ethical guidance to incorporate the legislative and regulatory realities of the online research environment.

6.3.5 The significant impact of law

By analysing the impact of legislation, regulation and online activities on online social research and the effectiveness of current ethical guidance to address and resolve this impact I was able to identify several key points:

- Legislation, regulation and online activities can have a profound impact on online social research practice.
- They directly affect online researchers as well as their participants.
- They pose difficult issues to the key areas of informed consent, confidentiality, anonymity and privacy and the safeguarding of the researcher and his subject.
- The issues that they bring about can be resolved by applying ethical principles, but current ethics guides are ill-equipped to deal with them.

- This is because they have not reflected upon the impact that legislation, regulation and online activities have on ethical considerations and research practice.
- Doing this is necessary to address the current tension between ethics and the law to ensure ethical and legal online social research.

Considering these key points, I can now argue that current ethical guidance has to be up-dated and extended in order to incorporate legislation, regulation and online activities. This is a continuous process to reflect the fast changing nature of the environment but is necessary to ensure that future online social research is legal and ethical.

6.4 Argument for an informed cyber ethics

The purpose of this chapter was to establish whether current ethical guidance was successful in guiding online social research or not in order to manage risk in online social research. The question I asked was "Can current ethical guidance successfully resolve the key issues identified in chapter five?" To achieve this purpose I first compared 'general' ethics guidance with online specific ethics codes. The rationale for this approach was that if the guides addressed the same ethical issues then we may only have to extend current ethical guidance to incorporate online issues. If they were providing radically different ethical issues and approaches to resolve them, then one may have to consider the need of entirely new ethics. The second half of the chapter then addressed the key ethical issues that arose out of the consideration of the impact of legislation, regulation

and online activities on online social research as identified in chapter five. It asked whether current ethical guidance can resolve those issues. The rationale for this approach was that if current ethics codes do address those particular issues and can resolve them, then we do not need new ethics. However, if they do not achieve this then we would have to design new ethics guides to incorporate the factors that have brought about their shortfall.

In summary the first part of the chapter provides evidence that allows me to argue that there are clearly marked differences between general and online specific research environments that pose questions for our ethical guidance. However, they do not pose new ethical issues. The conclusion I draw is that current general ethics codes need to be extended and up-dated in order to reflect on all the particular research environments in which social researchers are active. The second part of the chapter provides evidence that permits me to state that there is a readily identifiable gap in current ethical guidance. The gap is due to the complete oversight of pressing issues that arise due to the impact the legislation, regulation and surveillance activities in and of cyberspace and the Internet have on online social research practice. Based on this evidence I conclude that current ethical guidance has to be updated regularly in order to ensure that researchers remain legal and ethical in online social research environments.

Overall, I argue that we do not need new ethics, but new ethical guidance. By new I do not refer to creating new ethical issues, but providing a new framework

from which to address, assess and resolve ethical issues that incorporates the legal and regulatory realities of our research environments to ensure that our conduct is legal as well as ethical.

Chapter 7:

Managing the risks of online sociological research

7.0 Introduction

This thesis asks the question "how successful is current social research ethical guidance in managing potential risk in the context of online social research?" The key motivation and rationale for this study was that a) my initial research methodology identified a potential tension between ethics and the law that needed exploration; and b) a detailed literature review revealed considerable disagreement, ambiguity and gaps in the literature on, and guidance of online social research. This resulted in a library based study which moves from considering the research environment to its legislation and regulation and a reflection on their potential impact on online social research with the aim to establish whether current ethics guidance can resolve the issues identified in this thesis satisfactorily. The objectives of my thesis were to:

1) Identify dominant conceptualisations of the Internet and cyberspace as research contexts within social research.
2) Unpack the legal and regulatory conceptualisation of the Internet and cyberspace.
3) Document and analyse current legislation and regulations which are relevant to social research on/ or via the Internet and assess their potential impact on current research guidance and practice.

4) Critically evaluate ethical guidance in the context of the emerging legal and regulatory Internet and cyberspace to ascertain how suited they are to managing risk in online social research.

In this conclusion I begin by presenting the 'narrative' of the thesis displaying the whole structure of the thesis to show how chapters are connected and signpost my overall argument. While doing so I review how I have met the objectives of the thesis and contextualise what the outcomes of the investigation were to comment on my work's contribution to the field. Last but not least this chapter reflects on potential outcomes of the research findings for online social researchers their future research projects and provides a possible implementation framework.

7.1 Recapturing the narrative and methodology of my thesis

The thesis has taken a photographic approach to answering its main question. This approach was successful in that through moving from the wide-angle shot to the focused close-up it allowed taking account of all the key data sources and still produced a detailed and specific analysis. The methodology adopted in answering my research question employed two strategies. First it consisted of a library based research study that employed the tools of document analysis of legislation, regulation and ethics guidance and codes of practice via specific research schedules. Second, I identified and used hypothetical risks arising out of the

tension between the legal and regulatory reality of cyberspace and current social research practice to test current ethical guidance's ability to manage said risk.

Within this the thesis chapter one presents an overarching consideration of the interlinked matters of methods, ethics and the law that in there interplay impact on how social researchers construct and interact within a particular research environment. Chapters two and three outline the overall understandings of the Internet and cyberspace and outline the resulting claims made about them as research environments and online social research. Chapter four zooms in to consider how legislation, regulation and code shape cyberspace in ways not considered by social scientists. This leads to a further zooming in in chapters five and six where I identify emerging potential risks that the interplay between current research practice and the legal and regulatory reality of cyberspace bring about; to then use these as means to assess in how far current ethical guidance of social research can manage risks in online social research.

7.1.1 Is cyberspace new?

The argument of the thesis began in chapters one, two and three by revealing that there is considerable uncertainty and ambiguity surrounding online social research practice and guidance. This appeared to be the result of the dominant discourses focusing on 'newness' and 'difference' between online social research and 'traditional' forms of social research. Testing the merit of these claims on whether there is a genuine need for new research guidance for online social

research I began by focusing on the practical application of the research tool. I established that the Internet as a research tool is not a 'new' and 'different' paradigm but rather the result of the convergence of all the previously adopted technological tools into one. Chapters two and three further showed that the key difference is that the use of the Internet as a research tool is thought to move researchers and respondents from the real world into a parallel virtual one. This meant that it is not possible to purely assess the usefulness of current ethical research guidance on an analysis of the research tool. Instead, the need arose to consider this new and different research environment and to then assess whether current ethical research guidance is equipped to manage risk in online social research.

This is the chief aim of chapter three which critically engaged with the various fictional, political and academic conceptualisations of cyberspace and offered a consolidated understanding of it. The cyberspace that emerges out of these discourses is an extension of the offline world into an online world where the realities of the offline are amplified to the extreme. In such an amplified social space it is at this point difficult to predict in how far current social research ethics guidance can manage risk in online social research. What further made an assessment difficult was the fact that academic conceptualisations of social researchers are not considering the legal and regulatory framework of cyberspace sufficiently. This means that there is a considerable gap between the dominant

social theoretical conceptualisation of cyberspace and its actual legal, regulatory and coded reality.

To address this gap chapter four reveals the legal and regulatory conceptualisations of cyberspace. This chapter draws on the legal profession to supply social sciences with a grounded understanding of how cyberspace is actually created. This was done by scrutinising the literature on the regulation and legislation of the Internet and cyberspace to examine the ways in which legislation and regulation themselves either directly define the Internet and cyberspace or what kind of 'new' and 'different' sphere of social interaction their structuring of mediated social interaction creates. I was able to show that social research has to redefine cyberspace as a sphere based on legal, regulatory and coding structures that function as the active means by which cyberspace is created and maintained prior to any online social interaction taking place.

7.1.2 Is it risky?

The key matter throughout the thesis was that of risk, in particular, the potential risk that may emerge in cyberspace through social interaction or its legal and regulatory realities in general; and especially through our research activities within this context. Chapters two and three clearly identify that there is a shared recognition by everyone that there are potential risks that may emerge out of/ in cyberspace. Depending on the cultural, political, or academic starting point of the commentator these risks are more or less exaggerated than in the offline world.

Having established what kind of research space cyberspace is I considered the nature of the risk through a review of a large number of legislation and regulation in chapter five.

I was able to identify many potential legal-ethical issues that may emerge in everyday online social research practice. Regulations often mean that they either force the users of ISP services to act in certain ways or permit the ISPs themselves to take several actions, which were shown to be problematic for social research. In many cases this may mean that online social research is either prevented from using 'tried and tested' methods; that it may not be possible to meet ethical guidelines, or that research may not be carried out at all. Legislation's impact was shown to be played out mostly through the choice that a researcher has to apparently make in this legal context between being legal or ethical. This is because current legislation (and subsequent regulation) may at times undermine, bypasses, and thus make it almost impossible to fulfil our ethical objectives or methodological practice in the ways we are used to. Both regulation and legislations pose difficult issues to the key areas of informed consent, confidentiality, anonymity and privacy and the safeguarding of the researcher and his subject.

When reflecting on these findings my research clearly contradicts Kramarae's statement "…electronic communication at the moment exists almost completely outside of our legal universe" (Kramarae, 1995:15). Instead, they are much more

in line with the work by Olivero and Lunt (2004) and Jones whom I quoted earlier on "Ethics are not our only concern but also legal matters" (Jones, 2004:181). In the early part of the thesis I showed how little attention social scientists placed on the impact legislation and regulation have on online social research. Even if researchers do reflect on these matters the literature review suggests that they only consider those Acts included in their particular professional codes of conduct, and they do not engage with regulations at all.

Thus, I propose that the key reason that risk emerges in online social research is not because cyberspace poses some new ethical dilemmas, but rather, the fact that social scientists omit the legal and regulatory realities of cyberspace from their conceptualisation of this research environment and thus create a gap in their methodological and ethical considerations/ frameworks/ practice. It is the tension between ethics and the law that in any social research causes risk beyond the usual ethical dilemmas. When we now engage in an environment that is so heavily impacted on by legislation and regulation without considering them we amplify this tension tremendously. Thereby we actually exacerbate the actual risk posed by interacting in cyberspace. Thus, it is not cyberspace per se that is more risky than the offline research contexts, but social scientists' lack of understanding that leads to potentially incomplete ethical frameworks that makes cyberspace risky for online social research.

7.1.3 How well equipped are we to deal with the nature of these risks?

The above insight suggested that online social research ethical guidance was not well equipped in dealing with the potential risk of online social research. To study this in more depth and test this claim I reviewed a large number of current ethical frameworks and guidance and assessed their robustness by applying them to the risks identified in chapter five. The rationale for this approach was that if the sample of ethics codes and codes of practice are capable of resolving those issues by providing adequate guidance, there was no need to change them. The detailed analysis of each ethics code, the comparative analysis of online and offline ethics guides and applying them to the previously identified risks of online social research showed that here are clearly marked differences between general and online specific research environments that pose questions for our ethical guidance. However, they do not bring about new ethical issues. The issues that they bring about can be resolved by applying ethical principles, but current ethics guides are ill-equipped to deal with them. This is because they have not reflected upon the impact that legislation; regulation and online activities have on ethical considerations and research practice. Current ethical guidelines are inadequate in resolving the issues identified in chapter five because they do not incorporate the legal and regulatory reality of cyberspace into their frameworks. Therefore, current ethical guidance has to be updated regularly to ensure that researchers remain legal and ethical, producing high quality online social research. Doing this is necessary to address the current tension between ethics and the law to ensure ethical and legal online social research.

When reviewing these key findings in light of current literature used in this thesis they support the view that we need different ethical guidance for online social research. However, my research does not support the comprehensive replacement of current ethical guidance with entirely new and separate online social research ethics as demanded by amongst others Schneider and Foot (2005) and Siang (1999). Neither does my research sustain the views by Janowski and van Selm (2005), Jones (2004), Peden and Flashinski (2004) who question the value of online social research ethics. Instead the findings are far more supportive of the views offered by Thomas (2004) who writes "I argue that we need not invent new ethical rules for online research or try to reduce ethical behaviour in Internet research - or any other - … We need only increase our awareness of and commitment to established ethical principles (Thomas, 2004:187). However, Thomas (2004) and others like Denscombe (2005), and Hine (2005) while understanding that we do not need new ethics but revised ethical guidance, failed to identify the actual reason for this necessary revision. This is because they use their known and trusted approach to the matter at hand through ethical considerations of the new and different research environment. What they miss is the legal and regulatory realities of the research environment that makes the revision necessary.

7.2 Conclusion

In this thesis I set out to answer the question of "how successful is current social research ethical guidance in managing potential risk in the context of online social

research?" My research shows that current online social research guidance is insufficient in providing

(a) Information on the actual realities of the online research environment.
(b) Guidance on the legal and regulatory realities of cyberspace and their impact on online social research practice.
(c) Ethical guidance that enables the resolution of the impact of the legal and regulatory realities of cyberspace.

Therefore, in answer to the research question I argue that there is a need for continuously updated ethical guidance for online social research that is informed by a legal framework based on the legal and regulatory reality of cyberspace.

7.3 What does it mean?

7.3.1 Potential consequences for online social researchers

When considering these outcomes several potential consequences for current online social researchers may be suggested. The key message of this thesis is that online social researchers may no longer just simply rely on current professional codes of conduct, ethics codes or tried and tested methods. This is because they are not taking legislation and regulation of the Internet and cyberspace into account which results in potentially unmanageable risk in online social research. I propose that this leads to several more consequences.

From the beginning of their research project online social researchers will have to continuously identify and engage with the relevant legislation and regulation that applies to their particular online research environment. They then have to reflect on how they may adjust their ethical practice to overcome possible tensions between the identified legislation and regulation and their ethical approach.

Some researchers may also find that they cannot conduct their study due to the legislation and regulation that affects their research environment. This may mean that they have to considerably revise their research proposal; in the worst case scenario it may mean having to abort the project. Those online social researchers who are already undertaking research or have completed their study may well have to act retrospectively to comply with the relevant legislation and regulation that they had not taken into account previously.

Last but not least, my findings lead me to argue for an active involvement of online social researchers in debates about, and the actual creation of, legislation and regulation of the Internet and cyberspace. I would hope that that this will lead to social research practice being acknowledged in a way that avoids the tension between 'being ethical' and 'being legal'; enabling truly legal-ethical online social research in the future.

7.3.2 Moving on ideas

The overall contribution of my thesis can be split into four areas:

1) Offering a fundamentally re-conceptualised cyberspace through linking theoretical conceptualisations of cyberspace with its legal and regulatory reality thereby closing the conceptual gap persistent in current social theory.
2) Identifying potential risks that emerge our of cyberspace due to the tension between theoretical conceptualisations of cyberspace, resulting ethical practice and the legislation and regulation of cyberspace by analysing how legislation and regulation shape social interaction and thus research practice in cyberspace.
3) Identifying the legal-regulatory gap in current online social research guidance and practice through creating vignettes on which I tested the ability of current ethical guidance to manage the risks that they presented.
4) By the above offering a foundation for social research to create more appropriate research guidance and practice and thus a potential roadmap to legal cyber-ethics. Applying my findings within the framework set out in 'The concordat to support research integrity (Universities UK, 2012) will aid considerably in the achievement of its objectives in the field of online social research.

7.4 Future research opportunities

As this work is based on an analysis of codes of conducts and legislation and regulation and their implications for online social research the next step is to study how these implications are reflected upon and applied in approval processes of social research. Of particular interest are the ways in which current ethical guidance is actually applied/ interpreted by research councils or ethics boards (e.g. BSA, 2002). Specific questions to investigate are: Do they perceive shortfalls in the codes that they base their decisions and actions on and if so why do they identify these shortfalls?; and how do researchers then compensate for these? This is of interest because it may identify ethical practice that can manage risk in online social research that emerges out of social researchers' practical case by case responses to particular risks in online social research rather than being directly derived from ethics guidance; which then in turn may become the case study basis for updated social research guidance.

Another important undertaking is the creation of a continuously updated legal and regulatory database of cyberspace that provides an analysis of these in terms of their relevance and impact on online social research guidance and practice. To facilitate this task we need to build strong collaboration between lawyers, regulators and social scientists in order to ensure an appropriate identification and interpretation of legislation and regulation. This will thus result in a solid foundation from which social researchers can enter their chosen research space with appropriate methods, and legal ethical considerations and responses.

One further area to engage with is the perception of our research participants. Bakardjieva et al. (2004) and Bosnjak and Batinic (2002) have clearly identified that online users are very aware of online social research and have very strong views on covert research, informed consent and data protection. Therefore, engaging with these views is key in creating new forward looking ethical guidance in an online environment. I argue along these lines because our participants play an important part in creating cyberspace through their interpretation of the legal and regulatory reality and the possible social interactions within the thus created spaces of cyberspace. I propose that they built their own interpretation of morality and laws of online interaction that needs to be engaged with alongside our theoretical and legal regulatory realities in order to device ethical guidance and thus practice for online social research. Within this context answering the questions as identified on page 203 on harm, confidentiality and anonymity is especially important.

7.5 A roadmap to a legal-ethical framework for online social research

The thesis shows that the overall legal and regulatory environmental effect is that it is almost impossible to fulfil current ethical objectives when using current online social research practice and guidance. There is, therefore, a need for a regularly updated legal-ethical framework to inform our ethical considerations and practice when conducting online social research. While any social researcher may make immediate use of my thesis, particularly chapters five and six, to use the questions

and risks that I have identified to vet their own research considerations and activities, there is a much more advanced possible application of my thesis. I propose that it is not only possible but actually necessary to implement the key findings of my thesis into the framework of 'the concordat to support research integrity' (Universities UK, 2012) in order to achieve legal-ethical online social

7.5.1 Managing change

In order to facilitate the legal-ethical implementation framework within the 'concordat to support research integrity' I am drawing on and adapting common business practice, which has much experience in change management. This is of use here as my findings ultimately require the bringing about of change. Steps of change management include 1) establish the required change; 2) set strategic imperatives; 3) assess readiness of stakeholders; 4) devise change initiative; and 5) review and debrief (Cameron and Green, 2012).

7.5.1.1 The required change

The change I am referring to is born out of a need of risk management and entails the change of our conduct in online social research that is necessary to bring about legal-ethical online social research. This change is achieved by engaging with key stakeholders to implement my research findings in reflections on online social research practice and integrity. The underlying key activity then is defining cyberspace as framed by legislation and regulation; and cultivated through social interaction within this framework, which then leads to the explicit engagement

with relevant legislation and regulation to construct appropriate legal-ethical guidance and conduct.

7.5.1.2 The strategic imperatives

There are four strategic imperatives necessary to bring about this change.

1) Identify relevant stakeholders and their bespoke change initiatives.
2) Ensure that the key stakeholder (s) apply the findings of the research to their reflection on research integrity, especially the matter of managing risk in online social research.
3) The establishment of a common definition of cyberspace that draws on its legislative and regulatory realities while using social theory to explain actual social interactions and the perception of space within it.
4) Continuously update existing ethical guidance to reflect the legal and regulatory foundation of cyberspace.

7.5.1.3 Stakeholders and readiness

When considering stakeholders of online social research a considerable number of potential candidates come to mind. They include individual researchers (early career and established), universities and especially their ethics boards, professional associations, lawyers, local, regional and national governments. As Castells (1996) points out we are now living in a time where computer networks and society interact in complex ways to shape our lives. In order to understand

our technologically mediated lives and the emerging cultural and societal expressions we have to engage in the social study of online environments and the social interactions via or therein. This work is to be carried out by or under the direct guidance of individual researchers, study groups/networks, ethics boards, universities, professional associations. This makes them stakeholders in the implementation of the key findings of my thesis in order to create a legal-ethical framework for online social research that can identify and manage risk within the online research environment appropriately. While they all share an overarching interest they also hold a stake in particular facets. For example an individual researcher will not usually be concerned with devising training programmes on online research ethics, while a professional association or a university may well make that one of its key strategic imperatives.

The key stakeholders in this matter, however, are those institutions and associations that frame or manage the integrity of research. Here I refer to Universities UK, Research Councils UK and their component members, especially the Economic and Social Research Council (ESRC), and universities and professional associations such as the British Sociological Association. One of the key things that business practice addresses is that of 'organisational' readiness. This concept refers to having to identify who is affected by this change and are they ready to implement it. Often necessary change is identified by individuals outside or inside of organisations that then have to promote the ideas to others within an organisation or sector; rather than being the outcome of strategic

planning. In a way I am an outsider to the field. While I have undertaken my doctoral research in this area I am not an established and recognised online social researcher, nor am I a member of an ethics board, a university or professional association, nor a legislator or regulator. This means that individual researchers, their employers, funders or other organisations must be able to assess what their stake is in the roadmap to legal-ethical online social research guidance, and assess their own readiness and that of partners to implement strategic imperatives that are relevant to them in order to bring about the necessary change.

The assessment of readiness entails reflecting on: how important a change is perceived to be, what knowledge gaps and training needs arise, and required resources. While I consider the above imperatives to be crucial, universities, professional associations, research groups and even individual researchers may not share my sense of urgency. The latter is surprising considering the fact that the 'concordat to support the career development of researchers (2008, cited in Universities UK, 2012) actually requires researchers to take responsibility for recognising their role in keeping abreast of changing ethical, legal and professional obligations. One reason may be the associated cost in resources, time, and money that are required to establish new guidance, training and continuous review. More importantly, though, is the fact that the stakeholders that I identified thus far are not motivated. Evidence for this lies in the fact illuminated through my research that very few have actively strategically engaged with the matter of online social research ethics and thus its current lack of managing risk of

online social research. This affects our ability to bring about our strategic imperatives adversely and potentially prevents legal-ethical online social research.

7.5.2 Change making change possible

Recent developments in the research community, however, offer a real opportunity in achieving the strategic imperatives that I have outlined above. These include the Singapore Statement on Research Integrity (2010, cited in Universities UK, 2012) and the European Code of Conduct for Research Integrity (2011, cited in Universities UK, 2012). Both of these are concerned with the establishment of clear useful frameworks that inform our research practice and adhere to highest standards to manage risk in (social) research. In November 2012 Universities UK added its voice to this development when it published 'The concordat to support research integrity'. Signatories include all the key stakeholders in the framing of research activities such as the Department for Employment and Learning, the Higher Education Funding Council for England/ Wales, the National Institute for Health Research, Research Councils UK, Universities UK, Scottish Funding Council, and the Wellcome Trust. The purpose of the concordat is to build on "existing ethics processes, standards of professional practice and wider legal obligations" (Universities UK, 2012:7) to ensure research integrity. The concordat states that it:

> "[a]pplies to all fields of research, emphasises responsibilities and accountabilities, complements existing frameworks, and recognises the autonomy of employers. It then proceeds to consider five key

commitments that the research community has to sign up to and explains in detail how to achieve them. " (2012:10)

I studied the concordat in the context of my own research findings and was able to recognise a clear desire to support the kind of actions that are required to achieve legal-ethical online social research that I identified in my thesis. Examples include statements such as:

- "Conform to all ethical, legal and professional obligations incumbent on their work" (p.9)
- "strengthen institutional processes through training of researchers and more thorough reflections on the research environment." (p7)
- "Continue to monitor, and where necessary improve, the suitability and appropriateness of the mechanics in place to provide assurances over the integrity of research" (p.9)
- "Respect for the stewardship of research and scholarship for future generations" (p.11)
- "Employers have to : support researchers to understand and act according to expected standards , values and behaviours, and defending them when they live up to these expectations in difficult times. This includes supporting researchers to reflect best practice in relation to ethical, legal and professional requirements and having appropriate arrangements in place through which researchers can access advice and guidance on ethical, legal and professional obligations and standards." (p.12).

- "The frameworks that regulate research practice will change over time. Ethical concerns evolve and new legal obligations and professional standards are designated. There will, in many cases, be an international dimension. Therefore, it is not helpful to provide a single, definitive outline of the frameworks, standards, and obligations to which research must conform. However, all parties have a responsibility to ensure they have up-to-date knowledge or those that apply to their work" (p.13).

These key commitments of the concordat suggests that there has been a shift in focus recently that now enables the implementation of my research findings more readily into a legal-ethical online social research framework that can be brought about through the implementation of the commitments outlined in 'the concordat to support research integrity' (Universities UK, 2012). Thus, a new group of stakeholders transpires that one has to engage with who have a clear mandate and thus motivation to take ownership of the findings in this thesis to bring about a legal-ethical online social research framework that ensures research integrity through high quality practice. The specific stakeholders I identify are the concordat's own forum which consists of representatives of its signatories and meets to discuss research integrity matters; the UK Research Integrity Office; and then the individual signatories of the concordat itself. Not only does this provide a considerable range of resources and expertise it also provides us with stakeholders who have a vested interest, commitment and remit to take this forward.

7.5.3 First steps

Having identified the stakeholders and their 'readiness' in terms of stake in this matter I conclude my thesis with a suggestive first set of topics and questions for an initial agenda that may be addressed by the stakeholders.

1) How do you best provide researchers with training on the legislative and regulatory realities of the Internet and cyberspace?
2) What is the best way to keeping our knowledge of legislation and regulation of cyberspace up to date?
3) How do we best liaise with policing organisations to avoid compromising legitimate online social research?
4) How do we best come to terms with ethics in double data collection?

In the section above I have demonstrated how this thesis can be used in an applied way. Although application does not fall within the remit of the current project it offers many further possibilities for research into methodological questions surrounding online social research.

Appendix 1:

List of Legislation and Regulations analysed in the thesis

Laws: This list contains all the laws/Acts that were analysed. Not all appear in the thesis as only key examples were provided in evidence.

Data Protection and Privacy laws:

- **EU Data Protection Directives 1995, 1997, 2002**
- **EU Directive of personal data and the protection of privacy 1997**
- **EU Personal Data and Protection of Privacy 2002**
- **Personal Information Protection and Electronic Documents Act 2000 (CAN)**
- Privacy Act 1983 (CAN)
- **Data Protection Act 1998 (UK)**
- **Privacy Act 2005 (AUS)**
- **California Online Privacy Protection Act 2002/ 4 (US)**
- **Electronic Communications Privacy Act 1986 (US)**
- **Enhancement of Privacy and Public Safety in Cyberspace Act 2000 (US)**
- **Notification of Risk to Personal Data Act 2005 (US)**
- **Personal Data Privacy and Security Act 2005 (US)**
- **The Data Mining Moratorium Act 2003 (US)**
- **Securely Protect yourself against Cyber Trespass Act/Spy Act 2005 (US)**
- **Online Privacy Protection Act 2003 (US)**
- **Human Rights Act Article 8**

Security, Crime and Surveillance laws:

- **Convention on Cybercrime 2002/ 4 (EU)**
- **Creating a safer information society by improving the security of information infrastructures and combating computer-related crime 2002 (EU)**
- **Computer Misuse Act 1990 (UK)**
- Intelligence Services Act 1994 (UK)
- Terrorism Act 2000 (UK)
- Prevention of Terrorism Act 2005 (UK)
- Anti-Terrorism, Crime and Security Act 2001 (UK)
- **Regulation of Investigatory Powers Act 2000 (UK)**

- Police and Justice Bill 2005 (UK)
- Criminal Law Amendment Act 2001 (CAN)
- **Modernization of Investigative Techniques Act 2005 (CAN)**
- **Telecom Interception Capability Act 2002 (New Zealand)**
- Amendments to Homeland Security Act 2002 (US)
- **Communications Assistance for Law Enforcement Act 1994 (US)**
- Communications Decency Act –void after 1997
- Cybersecurity Enhancement Act 2002 (US)
- US Patriot Act 2001 (US)
- **Cyberspace Electronic Security Act 1999 (US)**
- **Fraudulent Online Identity Act 2004 (US)**
- The Computer Fraud and Abuse Act 2001 (US)
- **Internet Spyware Prevention Act 2004 (US)**
- No Electronic Theft Act 1997 (US)
- **Telekommunikationsueberwachungsordnung TKUV 2002 (GER)**
- **The Violence against Women and Department of Justice Reauthorisation Act 2005 (US)**
- Risk to Personal Data Act 2005 (US)
- The US Communications Assistance for Law Enforcement Act 1994 (US)
- Privacy and Public Safety in Cyberspace Act 1984/ 6/ 94/ 6 (US)
- Global Internet Freedom Act 2003 (US)

Children:

- Protection of Children Act 2003 (Scot)
- Children Act 2004 (UK)
- Jugendmedienschutz Staatsvertrag 2003 (GER)
- **Child Online Protection Act 1998 (US)**
- **Children's Online Privacy Protection Act 1998 (US)**
- **Deleting Online Predator Act 2006 (US)**
- **Prosecution Remedies and Tools against the Exploitation of Children Today Act 2002, 2003 (US)**
- Dot Kids Implementation and Efficiency Act 2002 (US)
- **Children's Internet Protection Act 2002 (US)**
- Child Pornography Protection Act 2002 (US) –rejected

- Child Abduction Prevention Act 2003 (US)
- Protection of Children Act 2003 (Scotland)
- Children Act 1989/ 2004 (UK)

Technology:

- Teledienstgesetz 1997 (GER)
- Telekommunikationsgesetz TKG 1996/ 7/ 8/ 2004 (GER)
- Zugangskontrolldienstschutz Gesetz 2002 (GER)
- Telecommunications Act 1997 (AUS)
- **Digital Age Communications Act 2005 (UK)**
- Fair, Transparent and Competitive Internet Naming Act 2003 (US)
- **Jurisdictional Certainty over Digital Commerce Act 2003 (US)**
- The Telecommunications Act 1996 (US)
- The Telecommunications Act 1997 (Australia)
- The Telecommunications Act 2002 (New Zealand)
- The Telecommunications Act 2004 (Spain)

Media Use:

- Global Internet Freedom Act 2003 (US)
- **Online Freedom of Speech Act 2005 (US)**
- **Digital Millennium Copyright Act 1998 (US)**
- Internet Tax Freedom Act 1998 (US)
- Video Voyeurism Act 2004 (US)
- **SPAM Regulation 2003 (EU)**
- **Controlling the Assault of Non-solicited Pornography and Marketing Act / Can SPAM Act 2003 (US)**
- Piracy Deterrence and Education Act 2004 (US)
- **Digital Age Communications Act 2005 (US)**
- **Internet Freedom of Speech Protection Act 2005 (US)**
- E-Commerce Gesetz ECG 2001(GER)
- Wettbewerbsrecht 2004 (GER)
- E-Commerce Gesetz ECG 2003 (Austria)
- Geistiges Eigentum Directive 2004 (EU)

Regulations:

- Keele University: Policy on Monitoring and Interception (February 2008)
- BT Privacy Policy (February 2008)
- Tiscali Privacy Policy (February 2008)
- Microsoft Online Privacy Statement (February 2008)
- Yahoo! Privacy and Cookie Policy (February 2008)
- Keele University: Computing and Information Systems Conditions of Use (February 2008)
- Yahoo! Terms of Service 2004-2007
- Microsoft Service Agreement (May 2007)
- Tiscali Acceptable Use Policy (February 2008)
- BT Terms of Service (February 2008)

Appendix 2:

Ethics codes and Codes of Practice

Ethics Codes and Codes of Practice: This list contains all the Ethics codes and Codes of Practice that were analysed. Not all appear in the thesis as only key examples were provided in evidence.

Government and Private Organisations:

- Government Research Unit 2006 (GSR)
- RESPECT 2004
- Barnardo's 2007
- Social Research Association 2003 (SRA)
- Economic and Social Research Council 2007 (ESRC)

Professional Associations:

- American Sociological Association 1999 (ASA)
- American Psychological Association 2002 (APA)
- British Sociological Association 1999, 2002 (BSA)
- International Sociological Association 2001 (ISA)
- British Society of Criminology 2000 (BSC)

Universities:

- Cardiff University (2006)
- Goldsmith College, University of London (2005)
- Keele University (2007)
- Kings College, University of London (2004)
- Lancaster University (2007)
- Leeds University (2004)
- Nottingham University (2000)
- University of Hull (2005)
- University of Kent (2005)
- University of Manchester (2007)
- University of Nottingham (2000)
- University of Southampton (2007)
- University of Surrey (2001)
- University of Sussex (2007)
- University of York (2006)

Online Ethics Guides:

- Association of Internet Researchers 2002 (AoIR)
- American Association for the Advancement of Science 1999 (AAAS)
- The National Committee for Research Ethics in Science and Technology 2003 (NENT)
- University of New Hampshire: Guidelines for conducting web-based survey research (2005)
- University of Sheffield (2003)
- University of Sheffield: The Internet: Accessing Human Participants and/or Data (2005)

Appendix 3:

Research schedules

Ethics research schedule:

Institution	
Ethics guide	
Date	

Question	**Data**
What is the purpose of this ethics guide?	
What particular approach is taken?	
What are the reasons given for taking this approach?	
What are the ethical issues addressed?	
How are they to be solved?	
Why are they to be solved in that way?	
Do they mention online research?	
Are traditional ethics applied to online research?	
How are traditional ethics applied to online research?	
Why are they applied in this way?	
Do online ethics differ from offline ethics?	
How do they differ?	
Why do they differ?	
What are the ethical issues of online research?	
How are they to be solved?	
Can they be solved satisfactorily?	
Is there a need to change traditional ethics in online context?	

Is the law mentioned?	

Why/ why not?	
What is cyberspace according to ethics guide?	
Does it differ from previous generation of ethics guides?	
Are there different rules for different places online?	
Who wrote it?	
Comments	

Law research schedule:

Country	
Law	
Date	

Question	**Data**
What area does the Act target?	
What does it legislate?	
What is its aim?	
Which agencies are involved?	
What powers do they have?	
What is permitted?	
What is forbidden?	
What is the punishment?	
Does it address online research?	
Does it make exemptions for research?	
What is the Act's impact on social research online?	
What does it mean for online methods?	
What does it mean for online ethics?	
What cyberspace emerges?	
Does this Act change others?	
How does this Act change others?	

Bibliography

Abate, J. (2003) "Popularising the Internet", in Communication History: Technology, Culture, Society, D. Crawley and P. Heyer (eds.), Boston: Pearson Education Inc.

Abercrombie, N. and Hill, S. and Turner, B. (2000) The Penguin Dictionary of Sociology, 4th edition, London: Penguin Books

Adams, L. (2003) 'Terrorists use internet to plot gang warfare', The Sunday Times, 16 February 2003.

Adler, P. and Adler, P. (2002) "Do university lawyers and police define research Values", in Walking the Tightrope: Ethical Issues for Qualitative Researchers, W. Van Den Hoonard (ed.), Toronto: University of Toronto Press.

Akeroyd, A.V. (1988) "Ethnography, personal data and computers: the implications of data protection legislation for qualitative social research", in Studies in Qualitative Methodology: Volume 1: Conducting Qualitative Research, R.G. Burgess (ed.), Stamford: Jai Press

Aktin, D.J. (2002) "Convergence across Media", in Communication, Technology and Society, C.A. Lin and D.J. Atkin (eds.), Cresskill: Hampton Press

Alderson, P. (1995) Listening to Children: Children, ethics and social research, Barnardo's

Alderson, P. (2000) Young children's rights: exploring Beliefs, Principles and Practice, London: Jessica Kingsley

Allen, C. (1996) "What's wrong with the 'Golden Rule'? Conundrums of conducting ethical research in cyberspace", available online at: http://venus.soci.niu.edu/~jthomas/ethics/tis/go.christin accessed 16/03/05

Allmark, P. (2002) "The ethics of research with children", in Nurse Researcher, December 2002

Anderson, W. (1998) SEXUAL HEALTH IN CYBERSPACE: Overcoming the obstacles to promoting sexual health on the internet. National HIV Prevention Information Service (NHPIS). London: Health Education Authority.

Armstrong, J. (2004) "Web Grrrls, guerrilla tactics" in Web.Studies, 2nd edition, D. Gauntlett and R. Horsley (eds.), New York: Arnold

Arnold, E.L. and Plymine, D.C. (2004) "Continuity with change: the Cherokee Indians", in Web.Studies2nd edition, D. Gauntlett and R. Horsley (eds.), New York: Arnold

Bachman, J.W. (2003) "The Patient-Computer interview: a neglected tool that can aid the clinician", in Mayo Clinical Proceedings, vol.78, (pp.67-78)

Bakardjieva, M. and Feenberg, A. and Goldie, J. (2004) "User-centred Internet Research: The Ethical Challenge", in Readings in Virtual Research Ethics: Issues and Controversies, E.A. Buchanan (ed.), London: INFOSCI

Banks, M. (2001) Visual Methods in Social Research, London: Sage Publications

Barlow, J.P. cited in Chesher, C. (1997) "The ontology of digital domains", in Virtual Politics: Identity & Community in Cyberspace, D. Holmes (ed.), London: Sage Publications

Barlow, J.P. cited in Loader, B.D. (1997) "The governance of cyberspace: politics, technology and global restructuring", in The governance of cyberspace, B. D. Loader (ed.), London: Routledge

Batinic, B. and Reips, U.D. and Bosnjak, M. (eds.) (2002) Online Social Sciences, Bern: Hogrefe & Huber Publishers

Bauman, Z. (1993) Postmodern Ethics, Oxford: Blackwell Publishing Ltd

Beck, U. (1992) Risk Society: Towards and New Modernity, London: Sage Publications

Benedikt, M. (1992) "Cyberspace, some proposals", in Cyberspace: First Steps, M. Benedikt (ed.), Cambridge: The MIT Press

Benedikt, M. (1992) "Cyberspace, some proposals", in Cyberspace: First Steps, M. Benedikt (ed.), Cambridge: The MIT Press

Best, S.J. and Kruger, B.S. (2004) Internet Data Collection, London: Sage Publications

Bober, M. (2004) "Virtual Youth Research: An Exploration of Methodologies and Ethical Dilemmas from a British Perspective", in Readings in Virtual Research Ethics: Issues and Controversies, E.A. Buchanan (ed.), London: INFOSCI

Borer, M.I. (2006) "The Cyborgian Self: Toward a critical social theory", available online at: http://reconstruction.eserver.org/023/borer.htm accessed 19/11/06

Bosnjak, M. (1997) Internetbasierte, computervermittelte psychologische Fragebogenuntersuchungen, St. Augustin: Gardez

Bosnjak, M. and Batinic, B. (2002) "Understanding the Willingness to Participate in Online Surveys: the case of e-mail questionnaires", in Online Social Sciences, B. Batinic, U.-D. Reips and M. Bosnjak (eds.), Bern: Hogrefe & Huber Publishers

Bostock, L. (2002) "'God, she's gonna report me': the ethics of child protection in poverty research", in Children and Society, vol. 16 (pp. 273-283)

Bryman, A. (2004) Social Research Methods, 2nd Rev Edition, Oxford: Oxford University Press

Buchanan, A.E. (ed.) (2004) Readings in Virtual Research Ethics: Issues and Controversies, London: INFOSCI

Buckle, S. (1993) "Natural law", in A companion to Ethics (Blackwell Companions to Philosophy), P. Singer (ed.), Oxford: Blackwell Publishers Ltd

Bush, G.W. (2002) cited in Administration of George W. Bush, available online at: http://books.google.co.uk/books?id=f_vhrnvPUqwC&pg=PA2127&lpg=PA2127&dq=the+department+will+gather+and+focus+all+our+efforts+to+face+the+challenge+of+cyber-terrorism&source=bl&ots=-cP72LO6lA&sig=JJxVmLQB3gSjTuCTjDu0s0jlgRw&hl=en&sa=X&ei=ukIrUfn7BYqYhQenoYCgBQ&ved=0CDsQ6AEwADgK#v=onepage&q=the%2

0department%20will%20gather%20and%20focus%20all%20our%20efforts%20to%20face%20the%20challenge%20of%20cyber-terrorism&f=false, accessed 24/09/2003

Butler, I. and Drakeford, M. (2005) Scandal, social policy and social welfare, 2nd edition, Bristol: Policy Press

Cameron, E. and Green, M. (2012) Making Sense of Change Management: a complete guide to the models, tools and techniques of organizational change, 3rd edition, London: Kogan Page

Castells, M. (1996) The Rise of the Network Society, Oxford: Blackwell

Castells, M. (1997) The End of the Millennium, The Information Age, Oxford: Blackwell

Castells, M. (1997) The Power of Identity, The Information Age: Economy, Society and Culture, Oxford: Blackwell

Castells, M. (2005) "The Network Society, from Knowledge to Policy", in The Network Society: from Knowledge to Policy, M. Castells and G. Cardoso (eds.), Washington: Johns Hopkins Center for Transatlantic Relations

Charles, S. (2005) Hypermodern Times, Cambridge: Polity Press

Chen, P. and Hinton, S.M. (1999) "Realtime Interviewing using the World Wide Web", in Sociological Research Online, vol.4, no.3, available online at: http://www.socresonline.org.uk/4/3/chen.html accessed 14/05/04

Chesher, C. (1997) "The ontology of digital domains", in Virtual Politics: Identity & Community in Cyberspace, D. Holmes (ed.), London: Sage Publications

Clarke, R. (2002) cited in "Clarke: Terrorists used Net for info on targets", available online at: http://articles.cnn.com/2002-02-15/tech/terrorists.internet.idg_1_terrorist-groups-qaeda-richard-clarke?_s=PM:TECH, accessed 18/02/02

Cohen, S. (2002) Folk Devils and Moral Panics, 3rd edition, London: Routledge

Coleman, M. (1996) Internet Detectives: Cyberfeud, : Macmillan Children's Books

Coleman, M. (1996) Internet Detectives: Net bandits, : Macmillan Children's Books

Collier, J. Jr. (1967) Visual Anthropology as a Research Method, Winston: Holt Rinehart

Coomber, R. (1997) "Using the Internet for Survey Research", in Sociological Research Online, vol.2, no.2, available online at: http://www.socresonline.org.uk/2/2/2.html accessed 14/05/04

Corden, A., Sainsbury, R., Sloper, P. & Ward, B. (2005) "Using a model of group Psychotherapy to support social research on sensitive topics", in International Journal of Social Research Methodology, vol. 8, no.2 (pp.151-160)

Corti, L. (2008) 'Issues in re-using qualitative data: the experience of Qualidata' in M. Dargentas, M. Brugidou, D. Le Roux et al. (eds.) L'analyse secondaire en recherche qualitative : une nouvelle pratique en sciences humaines et sociales (translation: Secondary analysis in qualitative research: a new practice in social and human sciences), Paris: Lavoisier. Collection: Tec & Doc.

Cotterrell, R. (1999) The Sociology of Law: an introduction, 2nd edition, London: Butterworths

de Beauvoir, S. (1949) Le deuxième sexe, Paris: Gallimard

de Montaigne, M. (2010) The Essays of Montaigne, :FQ Books

Denscombe, M. (2005) "Research Ethics and the Governance of Research projects: Potential of Internet Home Pages", in Sociological Research Online, vol.10, no.3, available online at: http://www.socresonline.org.uk/10/3/denscombe.html accessed 05/09/06

Derrida, J. (1981) Dissemination, Chicago: University of Chicago Press

Dingwall, R. (1980) "Ethics and ethnography", in Sociological Review vol.28, no.4, (pp.871-891)

Dodge, M. and Kitchin, R. (2001) Mapping Cyberspace, London: Routledge

Douglas, T. (2004) "Virus Writers: Sub-cultures", in Web.Studies, 2nd edition, D. Gauntlett and R. Horsley (eds.), New York: Arnold

DVRG (The Domestic Violence Research group) (2004) "Domestic violence and research ethics", in Researchers and their 'Subjects': Ethics, Power, Knowledge and Consent, M. Smyth and W. Williamson (eds.), Bristol: Policy Press

Easterbrook, F.H. (1996) "Cyberspace and the Law of the Horse", Symposium Presentation, University of Chicago Legal F 207

Ess, C. and AoIR (2002) "Ethical decision making and Internet research: Recommendations from the AoIR working Committee" available online at: http://www.aoir.org/reports/ethics.pdf accessed 04/05/2004

Fernback, J. (1999) "There is a there there", in Doing Internet Research, S. Jones (ed.), London: Sage Publications

Fowler, B. and Franklin, C. and Hyde, B. (2001) "Can you YAHOO!? The Internet's digital fences", in Duke L & Tech. Rev., 0012 available online at: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1009&context=dltr accessed 24/02/2013

Foy, G. (1996) The Shift, New York: Bantam USA

Gibbs, G.R. and Friese, W. and Mangabeira, W.C. (2002) "The use of new technology in Qualitative Research", in Forum Qualitative Sozialforschung, vol.3, issue 2, available online at: http://www.qualitative-research.net/fqs-texte/2-02/2-02hrsg-e.htm accessed 11/10/04

Gibson, W. (1984) Neuromancer, New York: Ace Books

Gibson, W. (1986) Burning Chrome, New York: Arbor House Publishing Company

Gibson, W. (1989). High tech high life: William Gibson and Timothy Leary in conversation. Mondo 2000, No. 7 (Fall), 58–64.

Giddens, A. (1990) The consequences of Modernity, Cambridge: Polity Press

Giddens, A. (1991) Modernity and Self-Identity: Self and Society in the Late Modern Age, Cambridge: Polity Press

Giddens, A. (1993) Sociology, 2nd edition, Cambridge: Polity Press

Gilbert, K. (2001) "Collateral damage? Indirect exposure of staff members to the emotions of qualitative research", in The Emotional Nature of Qualitative Research, K. Gilbert (ed.), Boca Raton, FL: CRC Press.

Gingrich, N. cited in Elmer-DeWitt, P. (1995) "Welcome to Cyberspace", in Time, special issue, vol. 145, issue 12, pp. 4-12

Goffman, E. (1959) The presentation of self in everyday life, London: Penguin Books

Goffman, E. (1963) Behaviour in Public Places: notes on the social organisation of gatherings, London: Collier-MacMillan

Goffman, E. (1971) Relations in Public: Microstudies of the Public Order, London: Penguin Books

Goldthorpe, J. et al. (1969) The Affluent Worker in the Class Structure, Cambridge: Cambridge University Press

Gore, A. cited in Chesher, C. (1997) "The ontology of digital domains", in Virtual Politics: Identity & Community in Cyberspace, D. Holmes (ed.), London: Sage Publications

Gozzi, R. Jr. (1994) "The Cyberspace Metaphor", in ETC: A Review of General Semantics, vol. 51, pp. 218-224

Greer, G. (1970) Female Eunuch, London: MacGibbon & Kee

Grinyer, A (2002) "The anonymity of research participants: assumptions, ethics and

Guest, T. (2007) Second Lives: A Journey through virtual worlds, London: Hutchinson

Guice, J. (1998) "Looking backward and forward at the Internet", in Information Society, vol.14, issue 3, (pp.201-222)

Hall et al. (2004) "'Need Help ASAP!!!': a feminist communitarian approach to online research ethics", in M.D. Johns ands.-L.S. Chen and G. Hall (eds.) Online Social Research: methods, issues & ethics, Oxford: Peter Lang

Harcourt, W. (2004) "World Wide Women and the Web", in Web.Studies, 2nd edition, D. Gauntlett and R. Horsley (eds.), London: Arnold

Harper, D. (2003) "Reimagining visual methods: Galileo to Neuromancer", in Collecting and Interpreting Qualitative Methods, N.K. Denzin and Y.S. Lincoln (eds.), 2nd edition, London: Sage Publications

Harvey, D. (1989) The Condition of Postmodernity, Oxford: Blackwell

Hekman, S.J. (1990) Gender and knowledge: elements of a postmodern feminism, Lebanon: Northeastern University Press

Herrera, D. (1999) "Two arguments for 'covert methods' in social research", in the British Journal of Sociology, Volume 50 issue 2, pp. 331-343

Hewson, C. et al. (2004) Internet Research Methods: A Practical guide for the Social and Behavioural Sciences, London: Sage Publications

Hillis, K. (1997) "Information technologies, subjectivities and space: virtual reality and social relations", Text of Speech, Geography Lecture Series, University of Colorado: Boulder

Hine, C. (2000) Virtual Ethnography, London: Sage Publications

Hine, C. (2004) "Social Research Methods and the Internet: A Thematic Review", in Sociological Research Online, vol.9, no.2, available online at: http://www.socresonline.org.uk/9/2/hine.html

Hine, C. (2005) "Virtual Methods and the Sociology of Cyber-Social-Scientific knowledge", in Virtual Methods: issues in Social research on the Internet, C. Hine (ed.), Oxford: Berg

Holge-Hazelton, B. (2002) "The Internet: A new field of qualitative Inquiry?", in Forum Qualitative Sozialforschung, vol.3, issue 2, available online at: http://www.qualitative-research.net/fqs-texte/2-02/2-02holgehazelton-e.htm accessed 11/10/04

Holloway, S. And Valentine, G. (2003) Cyberkids: children in the information age, London: RoutledgeFarmer

Homan, R. (1992) "The ethics of open methods" in British Journal of Sociology, vol. 43 (pp.321-332)

Homan, R. And Bulmer, M. (1982) "On the merits of covert methods: a dialogue", in M. Bulmer (ed.), Social Research Ethics, London: MacMillan Press

Hopkins, C. (2006) Cyber Cinderella, New York: 5 Spot

Illingworth, N. (2001) "The Internet Matters: Exploring the Use of the Internet as a Research tool", in Sociological Research Online, vol.6, no.2 available online at: http://www.socresonline.or.uk/6/2/illingworh.html accessed 14/05/05

Jackson, R. (2008) "Academic Freedom and the Study of Political Terror", available online at: http://sacrificialdevotionnetwork.wordpress.com/2008/06/18/academic-freedom-and-the-study-of-political-terror/ accessed 16/03/11

Janowski, N.W. and van Selm, M.V. (2005) "Epilogue: Methodological Concerns and Innovation in Internet Research", in Virtual Methods: Issues in Social Research on the Internet, C. Hine (ed.), Oxford: Berg

Jary, D. and Jary, J. (2005) Collins internet-linked dictionary of Sociology, 3rd edition, Glasgow: Collins

Johns, M.D. and Chen, S.-L.S. and Hall, G. (eds.) (2004) Online Social Research: methods, issues & ethics, Oxford: Peter Lang

Johns, M.D. and Hall, G.J. and Crowell, T.L. (2004) "Surviving the IRB review: Institutional Guidelines and Research Strategies", in Online Social Research: methods, issues & ethics, M.D. Johns and S-L.S. Chen and G.J. Hall (eds.), Oxford: Peter Lang

Johnson, D.R. and Post, D.G. (1996) "Law and Borders, the rise of law in cyberspace", in Stanford Law Review, available online at: http://www.cli.org/X0025_LBFIN.html accessed 05/05/06

Joinson, A. N. (2005) "Internet behaviour and the design of virtual methods", in Virtual methods: Issues in Social Research on the Internet, C. Hine (ed.), Oxford: Berg

Jonas, H. (1984) The imperative of responsibility: in search of an Ethics for the technological age, Chicago: University of Chicago Press

Jones, S. (2004) "Introduction: Ethics and Internet Studies", in Online Social Research: methods, issues & ethics, M.D. Johns and S-L.S. Chen and G.J. Hall (eds.), Oxford: Peter Lang

Josefsson.net (1994) "I don't even have a modem", available online at: http://josefsson.net/gibson/ accessed 08/02/2004

Kaczmirek, L. and Schulze, N. (2005) "Standards in online surveys: Sources for professional codes of conduct, ethical guidelines and quality of online surveys", available online at: http://websm.org/guides/ accessed 04/05/06

Kant, I. (1953) Groundwork of the Metaphysics of Morals, London: Harper

Karatzogianni, A. (2010) "The thorny triangle: Cyberconflict, business and the Sino-American relationship in the global system", in e-International Relations, available online at: http://www.e-ir.info/2010/03/10/the-thorny-triangle-cyber-conflict-business-and-the-sino-american-relationship-in-the-global-system/ accessed 24/02/2013

Katz, J. (1998) "The rights of kids in the digital age", available online at: http://www.wired.com/wired/4.07/features/kids.html accessed 07/09/03

Kendall, L. (1999) "Recontextualising 'Cyberspace': Methodological considerations for on-line research", in Doing Internet Research, S. Jones (ed.), London: Sage Publications

Kendall, L. (2004) "Participants and Observers in Online Ethnography: five Stories about Identity", in Online Social Research: methods, issues & ethics, M.D. Johns and S-L.S. Chen and G.J. Hall (eds.), Oxford: Peter Lang

Kitchener, K.S. and Kitchener, R.F. (2009) "Social Science Research Ethics: Historical and Philosophical issues" in The Handbook of Social Research Ethics, P.E. Ginsberg and D.M. Mertens (eds.), London: Sage Publications Inc.

Kitchin, R. (1998) Cyberspace: the world in the wires, Chichester: John Wiley & Sons

Kleinman, S.S. (2004) "Researching OURNET: a case study of multiple methods approaches", in Online Social Research: methods, issues & ethics, M.D. Johns and S-L.S. Chen and G.J. Hall (eds.), Oxford: Peter Lang

Knerr, C. R. (1982) "What to do before and after a subpoena arrives", in The Ethics of Social Research: Volume 1: Surveys and Experiments, J. E. Seiber (ed.), New York: Springer Verlag

Kramarae, C. (1995) "A backstage critique of virtual reality, in Cybersociety: Computer-mediated Communication and Community, S. Jones (ed.), Thousand Oaks: Sage

Krishnamurthy, S. (2004) "The Ethics of conducting e-mail surveys", in Readings in Virtual Research Ethics: Issues and Controversies, E.A. Buchanan (ed.), London: INFOSCI

Lax, S. (2004) "The Internet and Democracy", in Web.Studies, 2nd edition, D. Gauntlett and R. Horsley (eds.), Arnold: New York

Lee, N.M. (2001) Childhood and Society: growing up in an age of uncertainty, Buckingham: Open University Press

Lee, N.M. (2005) Childhood and Human Value: development, separation and separability, Buckingham: Open University Press

Lee, R.M. (1993) Doing research on sensitive topics, London; Sage Publications

Lee, R.M. (2004) "Recording technologies and the interview in sociology, 1920-2000", in Sociology, vol.38, no.5, London: Sage Publications

Leppard, D. (2003) 'Police will run internet after terrorist attack' . The Sunday Times, 15 June 2003.

Lessig, L. (1999) Code: and other laws of cyberspace, New York: Basic Books

Lin, C.A. (2002) "Communicating in the Information Age", in Communication Technology and Society, C.A. Lin and D.J. Atkin (eds.), Hampton Press: Cresskill

Loizos, P. (2000) "Video, film and Photographs as research documents" in Qualitative Researching: with text, image and sound, M.W. Bauer ad G. Gaskell (eds.), London: Sage Publications

Long, G.L. and Dorn, D.S. (1983) "Sociologists attitudes toward ethical issues: the management of an impression", in Sociology and Social Research, vol.67 (pp. 288-300)

Mann, C. and Stewart, F. (2000) Internet Communication and Qualitative Research: A Handbook for Researching Online, London: Sage Publications

Markham, A.N. (2004) "Representation in online ethnography: a matter of context sensitivity", in Online Social Research: methods, issues & ethics, M.D. Johns and S-L.S. Chen and G.J. Hall (eds.), Oxford: Peter Lang

Marshall, G. (1998) Oxford Dictionary of Sociology, Oxford: Oxford University Press

McDonough, J. (1995) "Being there: the use of cyberspace in computer-mediated communication", available online at: http://www.hayseed.net/MOO/cyberspace.ps accessed16/03/05

McGrory, D. (2003) 'Internet pervert who groomed girls jailed for 5 years'. The Times, 10 October 2003.

Midgley, M. (1993) "The origin of ethics", in A companion to Ethics (Blackwell Companions to Philosophy), P. Singer (ed.), Oxford: Blackwell Publishers Ltd

Millet, K. (1969) Sexual Politics, London: Granada Publishing

Mortishead, C. (2003) 'Internet pirates provoke identity crisis of luxury brands', The Times, 10 December 2003.

Murray, A.D. (2007) The Regulation of Cyberspace: Control in the Online Environment, New York: Routledge-Cavendish

National Statistics (2006) "Internet Access: Households and Individuals", available online at: http://www.statistics.gov.uk/pdfdir/inta0806.pdf accessed 03/08/07

Newman, M. (2008), "Researchers have no 'right' to study terrorist materials", Times Higher Education. 17 July 2008

Newman, M. (2009), "Reading lists inspected for capacity to incite violence", Times Higher Education. 25 June 2009

Newman, M. (2008), "Nottingham scholar held for 6 days under anti-terror law", Times Higher Education. 29 May 2008

Nunes, M. (1997) "What space is cyberspace?", in Virtual Politics: identity of community in cyberspace, D. Holmes (ed.), London: Sage Publications

Ó Dochartaigh, N. (2002) The Internet Research Handbook, London: Sage Publications

O'Neill, O. (1993) "Kantian ethics", in A companion to Ethics (Blackwell Companions to Philosophy), P. Singer (ed.), Oxford: Blackwell Publishers Ltd

Oakley, A. (1974) The sociology of Housework, Oxford: Martin Robertson

Olivero, N. and Lunt, P. (2004) "When the Ethics is functional to the Method: The case of E-Mail Qualitative Interviews", in Readings in Virtual Research

Ethics: Issues and Controversies, E.A. Buchanan (ed.), London: INFOSCI

Parmar, I. (2011) "Letter to VC", available online at: http://www.bisa.ac.uk/index.php?option=com_content&view=article&id=212&catid=25 accessed 08/12/11

Peck, R. (1995) Lost in Cyberspace, London: Puffin Books

Peck, R. (1996) The dream machine, London: Puffin Books

Peden, B. F. and Flashinski, D.P. (2004) "Virtual Research Ethics: A content analysis of surveys and experiments", in Readings in Virtual Research Ethics: Issues and Controversies, E.A. Buchanan (ed.), London: INFOSCI

Polsky, N. (1971) Hustlers, Beats and Others, Harmondsworth: Penguin

Porr, W.B. and Ployhart, R.E. (2004) "Organizational Research over the Internet: Ethical Challenges and Opportunities", in Readings in Virtual Research Methods: Issues and Controversies, E.A. Buchanan (ed.), London: INFOSCI

Poster, M. (1997) "Cyberdemocracy: The Internet and the Public sphere", in Virtual Politics: Identity & Community in cyberspace, D. Holmes (ed.), London: Sage Publications

Practicalities", in Social Research Update, Issue 36, Department of Sociology, University of Surrey

Preston, R. (1993) "Christian ethics", in A companion to Ethics (Blackwell Companions to Philosophy), P. Singer (ed.), Oxford: Blackwell Publishers Ltd

Punch, M. (1998) "Politics and ethics in qualitative research", in The Landscape of Qualitative Research, N. Denzin and Y. Lincoln (eds.) London: Sage Publications

Reips, U.D. (2000) "The web experiment method: advantages, disadvantages and solutions", in Psychological Experiments on the Internet, M.H. Birnbaum (ed.), New York: Academic Press

Rietz, I. and Wahl, S. (1999) "Vergleich von Selbst- und Fremdbild von PsychologInnen im Internet und auf Papier", in Online Research: Methoden, Anwendungen, und Ergebnisse, B. Batinic and A. Werner and l. Graef and W. Bandilla (eds.), Goettingen: Hogrefe

Ridge, T. (2001) cited in "Ridge in farewell speech, pledges to try to protect America's way of life", available online at: http://www.goerie.com/risingson/06.html, accessed 23/06/2004

Roberts et al. (2004) "Conducting Ethical Research Online: Respect for Individuals, Identities and the Ownership of Words", in E. Buchanan (ed.), Readings in Virtual Research Ethics: issues and controversies, London: Information Science Publishing

Rowe, C. (1993) "Ethics in ancient Greece", in A companion to Ethics (Blackwell Companions to Philosophy), P. Singer (ed.), Oxford: Blackwell Publishers Ltd

Sarup, M. (1988) An introductory guide to Post-Structuralism and Postmodernism, Hemel Hempstead: Harvester Wheatsheaf

Sassenberg, K. and Kreutz, S. (2002) „Online Research and Anonymity", in Online Social Sciences, B. Batrinic and U.D. Reips and M. Bosnjak (eds.), Seattle: Hogrefe & Huber Publishers

Savigny, F.K. von (1975) Of the Vocation of our Age For legislation and Jurisprudence, translated by A. Hayward, New York: Arno Press

Schneewind, J.B. (1993) "Modern Moral Philosophy", in A companion to Ethics (Blackwell Companions to Philosophy), P. Singer (ed.), Oxford: Blackwell Publishers Ltd

Schneider, M.S. and Foot, K.A. (2005) "Web Sphere Analysis: an approach to studying online action", in Virtual Methods: issues in social research on the Internet, C. Hine (ed.), Oxford: Berg

Selwyn, N. and Robson, K. (1998) "Using email as a research tool", in Social Research Update, issue 21 available online at: http://sru.soc.surrey.ac.uk/SRU21.html accessed 04/05/05

Siang, S. (1999) "Researching ethically with human subjects in Cyberspace", in Professional Ethics Report, 12 (4), available online at: http://www.aaas.org/spp/sfrl/per/per19.htm accessed 02/04/05

Sinha, I. (1999) The Cybergypsies, London: Scribner

Slack, R.S. (1998) "On the Potentialities and Problems of a www based naturalistic Sociology", in Sociological Research Online, vol.3, no.2, available online at: http://www.socresonline.org.uk/3/2/3.html accessed 25/05/04

Soja, E.W. (1996) Thirdspace: Journeys to Los Angeles and other real and imagined places, Oxford: Blackwell

Sommer, J. (2000) "Against Cyberlaw", in Berkeley Technology Law Journal, 15

Sontag, S. (2003) "On Photography", in Communication History: Technology, Culture, Society, D. Crowley and P. Heyer (eds.), Boston: Pearson Education Inc.

Speer, S.A. and Hutchby, I. (2003a) "From Ethics to Analytics: Aspects of Participants" orientations to the presence and relevance of recording devices", in Sociology, vol.37, no.2, London: Sage Publications

Speer, S.A. and Hutchby, I. (2003b) "Methodology needs Analytics: A rejoinder Martyn Hammersley", in Sociology, vol.37, no.2, London: Sage Publications

Speiglman, R. and Spear, P. (2009) "The role of Institutional Review Boards: Ethics: now you see them, now you don't" in The Handbook of Social Research Ethics, P.E. Ginsberg and D.M. Mertens (eds.), London: Sage Publications Inc.

Standage, T. (1999) The Victorian Internet, New ED edition, New York: Phoenix

Stern, S.R. (2002a) "Virtually speaking: Girls' self-disclosure on the www", in Women's Studies in Communication, 25 (2), 223-253

Stern, S.R. (2004) "Studying Adolescents Online: A Consideration of Ethical Issues", in Readings in Virtual Research Ethics: Issues and controversies, E.A. Buchanan (ed.), London: INFOSCI

Stone, R.J. (1991) "Virtual reality and cyberspace: from science fiction to science fact", in Information services and use, vol.11, (pp.283-300)

Sue, V.M. and Ritter, L.A. (2007) Conducting Online Surveys, London: Sage Publications

Sveningsson, M. (2004) "Ethics in Internet Ethnography", in Readings in Virtual Research Ethics: Issues and controversies, E.A. Buchanan (ed.), London: INFOSCI

Talbott, S.L. (1995) The future does not compute: Transcending the machines in our midst, Sebastopol, CA: O'Reilly

Taylor, T.L. (2006) Play between Worlds, London: The MIT Press

The Guardian (10th May 2011) "Letters: Call to Reinstate Terror Academic", available online at: http://www.guardian.co.uk/theguardian/2011/may/10/call-to-reinstate-terror-academci accessed on 20/05/11

Thomas, J. (2004) "Re-examining the Ethics of Internet Research: Facing the challenges of overzealous oversight", in Online Social Research: methods, issues & ethics, M.D. Johns and S-L.S. Chen and G.J. Hall (eds.), Oxford: Peter Lang

Thompson, K. (1999) "Social Pluralism and Post-Modernity", in Modernity and its Futures, S. Hall and D. Held and T. McGrew (eds.), Cambridge: Open University Press

Turkle, S. (1996) Life on the screen: Identity in the Age of the Internet, London: Weidenfeld and Nicholson

Universities UK (2012) The concordat to support research integrity. ISBN 978-1-84036-273-2. London: Universities UK.

Verton, D. (2003) Black Ice: the invisible threat of cyber-terrorism, Emeryville: McGraw-Hill

Virilio, P. (1989) "The Last Vehicle", in Looking back on the End of the World, D. Kamper and C. Wulf (eds.), New York: Semiotext

Walther, J.B. and Boyd, S. (2002) "Attraction to computer-mediated social support", in Communication, Technology and Society, C.A. Lin and D.J. Atkin (eds.), Cresskill: Hampton Press

Weber, M. (1990) The Protestant Ethic and the Spirit of Capitalism, London: Unwin Hyman

Weedon, C. (1994) "Feminism and the principles of post-structuralism", in Cultural Theory and Popular Culture: A reader, J. Storey (ed.), Hemel Hempstead: Harvester Wheatsheaf

Weitzmann, E.A. (2003) "Software and Qualitative Research", in Collecting and Interpreting Qualitative Materials, N.K. Denzin and Y.S. Lincoln (eds.), 2nd edition, London: Sage Publications

Weitzmann, E.A. and Miles, M.B. (1995) Computer Programs for Qualitative data Analysis, London: Sage Publications

Wheeler (2003) 'An amnesty for internet paedophiles? BBC News, 9 December 2003.

Williams, M. and Robson, K. (2004) "Reengineering Focus Group Methodology for the Online Environment", in Online Social Research: methods, issues & ethics, M.D. Johns and S-L.S. Chen and G.J. Hall (eds.), Oxford: Peter Lang

Williams, T. (1996) Otherland: Volume One; City of Golden Shadow, London: Orbit

Willmott, P. and Young, M. (1962) Family and Kinship in East London, Harmondsworth: Penguin

Online sources and websites:

Altcyberpunk.com, available online at: http://www.altcyberpunk.com

Cambridge Advanced Learners Dictionary, available online at: http://dictionary.cambridge.org

Heise Online, available online at: http://www.heiseonline.de/

Internet World Stats: Usage and Population Statistics, available online at: http://www.internetworldstats.com

Privacy International, available online at: http://www.privacyinternational.org

The Cyberpunk Project, available online at: http://project.cyberpunk.ru/idb/section_cyberpunk.html

Wikipedia, available online at: http://www.wikipedia.com

WordNet Dictionary, Princeton University Cognitive Science Laboratory, available online at: http://wordnet.princeton.edu/